“インターネット常時監視法＆サイバー版先制攻撃法”（案）だ！！

―「能動的サイバー防御法案」の危険性―

IT・インターネットの普及によりサイバー空間での不正なサイバー攻撃が大きな問題になっています。

例えば

米国では 2021 年石油パイプライン企業コロニアル・パイプラインが身代金目的でマルウエア（悪意のあるプログラム）を送り込むラムサムウエア攻撃の被害にあい５日間にわたり稼働を停止。

日本でも 2022 年トヨタ自動車系メーカーが攻撃を受けトヨタの国内工場が稼働を停止。2023 年名古屋港のコンテナ搬出入を管理するシステムがターゲットにされました。JＡＸＡ（宇宙航空研究開発機構）へのサイバー攻撃で情報の漏洩が。角川書店に対するサイバー攻撃で 1 か月以上収束できずグループ各社で多岐にわたり被害が。

サイバー犯罪に対する対処の高度化が求められています。

政府は「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」からの最終提言（2024 年 11/29）をうけ「能動的サイバー防御法案」を閣議決定し今通常国会に提出しました（2025 年 2/7）。

「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（新法）」

「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」（整備法）です。

でも提出された法案は“インターネット常時監視法案”であり、”サイバー版先制攻撃法案“で、国民の基本的人権が否定され、サイバー版敵基地砲撃を当たり前とする軍事化の社会になってしまいます。

内容を見ていきましょう。

「新法」では“官民連携”“通信情報の利用”が規定され、「整備法」で警察官職務執行法の改正・自衛隊法の改正などで“アクセス・無害化措置”について規定されています。

能動的サイバー防御とは

「武力攻撃事態に至らないものの、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恐れがある場合これを未然に排除し、又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」ことです。（日経ビジネス）

そのための「アクセス・無害化」とは、

攻撃元となるサーバ（国外・国内）にアクセスし、攻撃能力を持つプログラムを停止・解除する＝サイバー攻撃をすることです。

サーバが国外にある場合には他国の“主権を侵害する”という問題があり、NATO 関係の「タリン・マニュアル 2．0」でもその主権侵害の違法性を阻却する事由が必要であるとしてルール化しています。

すなわち「国家は根本的利益に対する重大で差し迫った危険を示す行為への反応としてそうすることが当該利益を守る唯一の手段である場合」と厳しい要件を付しています。

今回の法案ではこのような厳しい要件は規定されていません。法案の内容を見てみましょう。

〇国に対して”警察と自衛隊によってアクセス・無害化＝サイバー攻撃をする“権限が与えられています。

〇無害化を実行できるのは「サイバー攻撃またはその疑いがある通信等を認めた場合であって、そのまま放置すれば人の生命・身体・または財産に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」です。

≪警察が実施する場合≫

“警察庁長官が指名する警察官（サイバー危害防止執行官）”が、サイバー等の管理者への措置命令、あるいはみづから危害防止のため電気通信回線を介して措置をとることができます。

サイバー危害防止措置執行官は警察庁長官又は、都道府県警察本部長の指揮下で、事前に独立機関「サイバー通信情報監理委員会」の承認を得て実施するのです。（いとまがないときは事後に通知）

対象電子計算機が国外に設置されている場合は、警察庁長官を通じて「外務大臣」と協議をする。

この権限は「警察官職務執行法改正６条の２」によって与えられるのです。

＊警察庁にはサイバー犯罪の「捜査権」と、今回の「能動的サイバー防御＝サイバー攻撃権」を与えられるまでになっています。戦後警察庁には捜査権もなかったのですがサイバー犯罪に対応するといって捜査権も攻撃実行権も与えられました・・・この意味するところは？

≪自衛隊が対処する対象は≫

「国の行政機関や地方公共団体、基幹インフラ、一定の防衛産業が使用する重要な電子計算機に対する「特定不正行為」で外国勢力による特に高度に組織的かつ計画的なものが行われた場合において、自衛隊が対処する特別の必要があると認めるとき、内閣総理大臣が当該電子計算機に対する“通信防護措置”をとるべき旨を命じることができる。」のです。

根拠法は自衛隊法改正案第 81 条の３、第 91 条の３、第 95 条の４によって（整備法案）。

実施は自衛隊の部隊が“警察と共同対処”です。

措置の実施には防衛大臣の指揮を受ける。警職法改正法を準拠しての対処です。

もう少し詳しく自衛隊が実施できる要件を法案から明らかにしましょう。

特定不正行為とは

① 不正アクセス禁止法が定める不正アクセス

② 刑法 168 条の２「不正指令電磁的記録作成等第２項。

③ 刑法第 35 章が罪とする行為
であり、

以上の行為によって、更に以下の３要件をすべて満たした場合に限って首相が通信防護措置を命じるのです。

1, 国家及び国民の安全を著しく損なう事態が生じる恐れが大きい。
2, 自衛隊が保有する特別の技術または情報が必要不可欠。
3, 国家公安委員会からの要請または同意がある。

外国にある電子計算機に対処するときは防衛大臣を通じて「外務大臣」と協議する。そして「サイバー通信情報監理委員会」の事前承認が必要です。（いとまがないときは事後の通知）

○更に自衛隊の部隊は

“自衛隊または在日米軍が使用する電子計算機をサイバー攻撃から業務上警護する”自衛官も改正警職法の権限を準用する。そして「武器等防護」（平時において自衛隊自身や自衛隊と連携して日本の防衛に資する活動に従事する米軍などの武器を防護する任務）においても必要な時は「無害化」を実行可能とするのです。

以上みてきたように「能動的サイバー防御」とはサイバー空間のサイバー攻撃を未然に防ぐためとはいえ、他国（サイバー攻撃の 99%が海外のサーバから）のサーバを攻撃することで無害化するので、これは他国への主権侵害に当たることは明らかです（「タリン・マニュアル」からも明らか）

果たして“緊急避難の法理”を使えるのだろうか？非常に疑問です。

又、防衛予算に計上されている（2025 年度 2927 億円）自衛隊の行動としてのサイバー領域での整備・対処・防御・攻撃と、今回の法案「能動的サイバー防御法案」での他国へのサイバー攻撃（無害化）との線引きは？

武力攻撃事態（有事）は自衛隊が軍事的に対応するのでしょうが、法案の対象は“武力攻撃事態にいたらない「重要影響事態」「存立危機事態」＆平時”を対象とするものとしてもその堺が分かりません。

警察と自衛隊が共同で対処することで警察の軍事化、自衛隊の警察化にもなってきます。（いいのだろうか？）

海渡雄一弁護士も指摘するように無害化の対処は“サイバー版の先制攻撃”であり、これを法定化することは認められないのでは・・・あまりにも危険な法案です。

サイバー空間の通信情報の秘密は守られるか？

この危険極まりない無害化＝サイバー攻撃（能動的サイバー防御）をするためにサイバー空間の情報を監視・検索することを認める法案が“官民の連携”と“通信情報の利用”を規定した「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」です。

ではこの法案によって認められようとしている通信情報の監視・利用が果たし

て憲法21条「通信の秘密」「表現の自由」、19条「内心の自由」との関係で許されるのか検討してみましょう。

「最終提言」では「サイバー攻撃実態の把握のための通信情報利用が必要だ」「被害を未然に防止するためには通信情報を分析することによりボットやC2サーバで構成される攻撃用インフラの実態を把握し防御を可能にすることが必要であり、特にアクセス・無害化を行うに当たっては今まで以上にサイバー攻撃に関する詳細で十分な量の観測・分析の積み重ねが必要である」と説いています。これを実現するために新しい法律でサイバー空間の情報の監視・検索そして利用の仕組みが規定されています。

官民連携の強化として

○基幹インフラ事業者は特定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に「届け出」をし電子計算機のインシデント情報やその原因となりうる事象を認知したときは事業所管大臣及び内閣総理大臣に「報告」を義務付け（新法4条・5条）。

○内閣総理大臣により「情報共有及び対策に関する協議会」が設置され、基幹インフラ事業者、電子計算機等のベンダー等をその同意を得て構成員として加える（守秘義務あり）。そして情報共有をする。重要電子計算機にもちられる電子計算機の脆弱性を認知したらベンダー等へ情報を提供。

通信情報の利用について

官民連携の体制を作ったうえでサイバー攻撃の実態を把握するため通信情報の利用、分析について新たな法律が規定しています。

“サイバー攻撃の99%は海外からの発信”との認識の上、外外通信（国内を経由し伝送される国外から国外への通信）、外内通信（国外から国内への通信）、内外通信（国内から国外へ通信）の情報を取得するとのことです。

≪同意に基づく取得≫

内閣総理大臣は基幹インフラ事業者との協定（同意）に基づき、外内通信にかかる通信情報を用いて分析を実施。事業者に分析結果を提供。

≪同意によらない情報の取得≫

外外通信の取得：内閣総理大臣は国外の攻撃インフラ等の実態把握のため必要と認めた場合独立機関（サイバー通信情報監理委員会）の承認を受け通信情報を取得。

外内・内外通信の取得：内閣総理大臣は国内へのサイバ攻撃の実態把握のため特定の外国設備との通信を分析する必要があると認める場合「サイバー通信情報監理委員会」の承認を受け通信情報を取得。

≪取得した情報は…≫

取得情報につて“人による知得を伴わない自動的な方法”により調査すべきサイバー攻撃に関係があると認めるにたる“機械的情報（本質的内容でない情報）”を選別する。

果たして能動的サーバー防御をするためという理由で本法案規定のように基幹インフラ（電気・ガス・水道・航空・金融・港湾・郵便・運輸など15種のイ

ンフラ）や重要物資のサプライチェーンのサイバー空間の情報、政府・自治体、機微情報を保有する事業者、機器ベンダというほぼあらゆる領域のサイバー空間での通信情報の監視と利用が許されるのだろうか？

通信傍受法（盗聴法）でも令状が必要なのに、令状一つも必要なく、事業者の同意がなくても「監理委員会」の承認を得れば通信情報を監視・使用するのは憲法 21 条が保証する通信の秘密に抵触し、プライバシー侵害につながる懸念があります（海渡雄一弁護士）。

政府の本法案の説明では、意思疎通の本質的な内容でない機械的な情報だけを利用するといっているが、本質的内容でないものの中にメールアドレスも入っています。“送信者の氏名・住所・電話番号・発信受信場所・通信日時・時間・回数も通信の秘密に含まれる”ということはこれまでの裁判判決（東京地裁平成 14 年 4/30 判決）からも明らかです（海渡双葉弁護士）

又、収集対象は外外、外内、内外通信であって“内内”通信は対象外と言っているが、提言で説明されているように“最初は広く、懸念が見つかったら深く”なので内内通信が確実に除外されるとは規定されていないのです。

サイバー空間での通信情報の取得に関するドイツ連邦憲法裁判所の判決が 2024 年 10 月 8 日に出されています。“サイバー脅威を探知する目的で国際電気通信の戦略的監視を行う連邦情報局の権限は部分的には違憲と判断されました。その理由は①私生活の核心の傍受は許されないといっているのにこの点について十分具体的に規定されていない②国内通信のデータ削除に関する十分具体的な制度機規定が欠けている。と。

ドイツでの判決内容が日本の今回の法案で検討されているとは思えません。

日本政府も衆議院予算委員会で「通信の秘密につても公共の福祉の観点から必要やむを得ない限度において一定の制約に服すべき場合がある」（内閣法制局）と答弁し公共の福祉の観点から能動的サイバー防御は容認されるといっています。

しかし、公共の福祉の観点というなら国民一人一人の基本的人権（憲法 21 条・19 条）とその侵害との比例原則から適正なのかどうかが問題となります。ドイツの憲法裁判所でも厳しくその規定の仕方に問題を指摘しています。厳格であるが上にも厳格に規定されなければならないはずですが・・・

サイバー攻撃を防ぐためという目的のために日常生活のあらゆる領域のサイバー空間の通信情報を取得するのは、かつてスノーデンが指摘した米国が行っていた“コレクトイットオール”そのものです。

まさに海渡弁護士が言うように今回の法案は「令状なき常時インターネット監視法」です。

能動的サイバー防御法案は撤回を！

今回の「能動的サイバー防御法案」の二つの側面「令状なき常時インターネット監視法」＆「サイバ-版先制攻撃法」からして法案の撤回が必要です。

今、目の前にあるサイバー攻撃の防御のためにはより精度の高い防御システム

を作り上げ、更に国際社会の中でサイバー攻撃に対しあらゆる国が非難する体制づくりが必要なのではと思われます。これが急務の課題のはずです。

今回の法案は安保３文書「国家安全保障戦略」、そして経済安保の「経済安全保障推進法」「経済秘密保護法（セキュリテイクリアランス法）」と一体のものとして出されてきているもので軍事だけでなく経済領域でも米国の世界戦略と一体化して日本の安全保障政策を推進していこうとするものです。

又、法案に規定されている内閣官房（指令塔・総合調整）に新設されるサイバセキュリテイの確保に関する総合調整の事務を掌理する“内閣サイバー官”は、その組織としてCIA のような組織になっていくのではと懸念されています。（海渡）

「警察官職務執行法の改正」「自衛隊法の改正」で「能動的サイバー防御」を実施していこうとするこの法案は、“警察の自衛隊化”と“自衛隊の警察化”そして“自衛隊の米軍と一体的に行うサイバー防御・攻撃戦略”とまさに平時～有事とシームレスな能動的サイバー防御・攻撃体制を作ろうとしていることが明らかになっています。

戦時体制の法体系がまたまた作られようとしているのです。“安保法制（集団的自衛権行使）”“安保３文書（敵基地攻撃能力・GDP2%軍拡予算）”“経済版2+2”と大きな日米一体化の流れの中での「能動的サイバー防御法案」なのです。

もうこれ以上の「軍事化」そして国民一人一人の個人の尊厳を否定する「監視社会」への流れをストップさせましょう！！

「能動的サイバー防御法案」反対！！

＊「民主主義と自治そして平和主義」藤代政夫　047-445-9144

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 及び 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　概要

内閣官房サイバー安全保障体制整備準備室

趣　旨

○　国家安全保障戦略（令和４年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**内閣サイバーセキュリティセンター（ＮＩＳＣ）の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置**等の実現に向け検討を進めるとされた。

○　国家安全保障戦略に掲げられたこれら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、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を開催（令和６年６月７日～11月29日）、「サイバー安全保障分野での対応能力の向上に向けた提言」を取りまとめ。

→　これらを踏まえ、「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」（新法）及び「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」（整備法）として必要な法制度を整備。

概　要

官民連携（新法）

○基幹インフラ事業者による
・導入した一定の電子計算機の届出
・インシデント報告

○情報共有・対策のための協議会の設置

○脆弱性対応の強化

等

通信情報の利用（新法）

○基幹インフラ事業者等との協定（同意）に基づく通信情報の取得

○（同意によらない）通信情報の取得

○自動的な方法による機械的情報の選別の実施

○関係行政機関の分析への協力

○取得した通信情報の厳格な取扱い

○独立機関による事前審査・継続的検査

等

分析情報・脆弱性情報の提供等

アクセス・無害化措置（整備法）

○重大な危害を防止するための警察による無害化措置

○独立機関の事前承認・警察庁長官等の指揮

等（警察官職務執行法改正）

○内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）

○自衛隊・在日米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等（整備法）

○サイバーセキュリティ戦略本部の改組　（サイバーセキュリティ基本法改正）
○サイバーセキュリティ戦略本部の機能強化　（サイバーセキュリティ基本法改正）
○内閣サイバー官の新設　（内閣法改正）　等

施行期日

公布の日から起算して１年６月を超えない範囲内において政令で定める日　等

（社会新報２月２０日号２面より）

福島党首 と海渡双葉弁護士

2025/02/16

社民党の福島みずほ党首はこのほど、『月刊社会民主』３月号の企画で、秘密保護法対策弁護団事務局長の海渡双葉弁護士と対談。能動的サイバー防御（ＡＣＤ）法案の危険性について語り合った。対談の全文は近日発売の月刊社会民主に掲載される。

ＡＣＤ法案は、警察や自衛隊等の政府機関が常時メール等の通信を無制限に監視・収集し、サーバーに侵入して「無害化」（＝破壊）するというもの。７日に閣議決定され、通常国会に提出された。福島党首と海渡弁護士は、これは憲法２１条が保障する「通信の秘密」の侵害につながり、最悪の場合には戦争の引き金にすらなり得ると危惧する。

政府が設置した有識者会議は、ＡＣＤについて昨年１１月に提言を発表。増加しているサイバー攻撃に対処するためのものとの建前はあるが、２月７日に閣議決定された法案の内容が憲法で保障された「通信の秘密」とプライバシーを侵害することは明白だ。

海渡弁護士は「プライバシー侵害で反対運動が盛り上がった通信傍受法（盗聴法）ですら、犯罪の可能性、容疑があるとして令状を取ってそれで電話を盗聴するというものだった。しかし、今回のＡＣＤ法案は何か犯罪の予兆があるからではなく、裁判所の令状なし、つまり裁判所の審査をなしに警察や自衛隊が常時、ネット監視するものだ」と批判した。

福島党首は、岐阜県の大垣市での市民運動を警察が徹底的に監視していた事件について語った。

この事件は、岐阜県での大型風力発電施設の建設計画について問題点を考える勉強会を市民が開催したところ、県警が参加者の個人情報を収集した上、事業者側に提供したというもの。市民側は損害賠償や個人情報の抹消を求めて提訴。昨年９月に名古屋高裁で勝訴した。

海渡弁護士はこの判決について「個人情報の収集・保管・外部への提供はいずれも違法と判断した。個人情報の収集が憲法で保障された表現の自由や内心の自由に対する間接的な制約になると判断された」と指摘し、ＡＣＤ法案と共通する問題点を強調した。

ＡＣＤ法案のもう一つの問題点は「外国がサイバー攻撃を仕掛けてくる兆候がある」と警察や自衛隊が判断した場合、未然に外国のサーバーを「無害化」すること。福島党首は「これはサイバー版敵基地攻撃能力ではないか」と指摘。海渡弁護士も「外国の主権を侵害してサーバーを『無害化』する場合、英国では、国務大臣の許可状がいる。オーストラリアでは令状を取らなければいけない。カナダでは、国防大臣が許可を発出するのですが、外務大臣の要請または同意があった場合に限って許可できる」と例示。それに対して日本は「独立機関の承認だけで警察と自衛隊が行なう」として、あまりに安易にＡＣＤを運用しようとしていることに懸念を表明した。