サイバー戦争へ踏み込む日本-安保三文書の意味とは(2023/10/20院内集会)

Table of Contents

1. はじめに

「(共同声明)能動的サイバー防御と関連する法改正に反対します―サイバー戦争ではなくサイバー領域における平和を」の内容を紹介しながら、「サイバー戦争」の問題を考えます。

2. 2022年12月に安保防衛三文書が閣議決定された。この文書に「能動的サイバー防御」という言葉が登場した。

2.1. 能動的サイバー防御とは何なのか

ここには、「可能な限り未然に攻撃者のサーバー等への侵入・無害化できるよう、政府に対し必要な権限が付与されるようにする」「サイバー安全保障分野における新たな取り組みの実現のために法制度の整備、運用の強化を図る」(「国家安全保障戦略」)などと明記された。

国家安全保障戦略では、次のように何らの説明もなしに突然「能動的サイバー防御」という言葉が登場する。

> 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。

能動的サイバー防御は武力攻撃の有無とは関係なく、行使されるということだ。能動的サイバー防御もまたサイバー領域における武力行使であるだけでなく、先制攻撃を公然と主張したことになる。

2.2. 経団連の説明会

経団連が4月に開いた改定安保3文書に関する説明会で、内閣官房サイバー安全保障体制整備準備室の小柳誠二室長は、能動的サイバー防御について以下のように説明した(経団連のウエッブ)

> 武力行使に至らないものの、国や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、当該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。サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御を実施し得る体制を整備するため、以下（1）～（3）を含む必要な措置の実現に向けて検討を進める。
>
> （1）民間事業者等がサイバー攻撃を受けた場合の政府との情報共有や、政府から民間事業者等への対処調整、支援等の取り組み強化
> （2）国内通信事業者が役務提供する通信にかかる情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するための所要の取り組み
> （3）国や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、

> 政府に必要な権限を付与
> https://www.keidanren.or.jp/journal/times/2023/0420_04.html

特徴的なことは民間業者との連携の強化であり、通信事業者が保有する「情報」の活用が強調されているこだ。サイバー以外の軍事安全保障ではみられないことだ。

2.3. 能動的サイバー防御の範囲は従来の自衛隊の任務を大きく逸脱する

私たちの生活の基盤は、電力、交通、医療、金融まで、情報通信システムなしには機能できない。情報通信システムはコンピューターのネットワークによって機能しており、インターネットはその中核的な仕組みとして世界中をひとつのネットワークとして繋ぐ仕組みとなっている。サイバー安全保障は国家安全保障の一部だが、「安保戦略」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」と述べることで、事実上憲法9条による戦争放棄条項が国家に要請する安全保障上の制約を捨て去った。

3. サイバー領域（インターネットやコンピュータネットワークおよびこれらを用いたコミュニケーション環境のこと）において軍事を最優先させる政策は、サイバー領域全体を戦争に巻き込み、私たちのコミュニケーションの権利を根底から脅かすことになる。

3.1. 2019年 安保条約5条の解釈が変った

2019年に日米安保条約の対象領域に「サイバー」を追加した。 NHK報道
https://www.nhk.or.jp/politics/articles/statement/16854.html https://www.asahi.com/articles/ASM4M544BM4MUTFK01J.html

> 閣僚は，国際法がサイバー空間に適用されるとともに，一定の場合には，サイバー攻撃が日米安保条約第５条の規定の適用上武力攻撃を構成し得ることを確認した。
> 出典：日米安全保障協議委員会共同発表 https://www.mofa.go.jp/mofaj/files/000470737.pdf

安保条約第5条とは以下である。

> 各締約国は、日本国の施政の下にある領域における、いずれか一方に対する武力攻撃が、自国の平和及び安全を危うくするものであることを認め、自国の憲法上の規定及び手続に従つて共通の危険に対処するように行動することを宣言する。
> 　前記の武力攻撃及びその結果として執つたすべての措置は、国際連合憲章第五十一条の規定に従つて直ちに国際連合安全保障理事会に報告しなければならない。その措置は、安全保障理事会が国際の平和及び安全を回復し及び維持するために必要な措置を執つたときは、終止しなければならない。

3.2. サイバー領域での日本の役割は、より積極的になる

サイバー攻撃が上の5条にいう「武力攻撃」に含まれる、という解釈の変更を踏まえて、「安保戦略」の能動的サイバー防御があることを忘れていはならない。米軍が一方的に日本の防衛に関与するかのような前提はサイバー領域では成り立たない。つまり、日本はより積極的に自らサイバー攻撃の主体となって米国と共同行動をとる可能性が高い、ということだ。他方で、米国は日本国内のサイバー領域への諜報活動や監視などにも関与することが今まで以上に容易になる。しかし、こうしたサイバー領域での軍事行動はほとんど可視化されない可能性がある。

4. 政府は**2023**年**1**月**31**日に、一元的サイバー安全保障体制整備準備室を内閣官房に設置し、今後必要な法改正を検討する。

この準備室についての情報がほとんどでてこない。上述のように、経団連は4月に「改定安保3文書に関する説明会」を開催し、ここに内閣官房サイバー安全保障体制整備準備室の小柳誠二室長が参加しているが、ウエッブ上の記事では、「安保戦略」文書の説明以上のものはない。強調されえいるのは、民間との協力と内閣サイバーセキュリティセンター（NISC）の権限強化である。NISCの権限強化とは民間企業への強制力をもたせるということだ。プロバイダーなどを政府のスパイ行為やサイバー攻撃に強制的に動員させられる体制を構築することが目論まれている。

また、安保防衛三文書をみると自衛隊だけでなく、政府全体の統治機構の改編が予定されていることがわかる。

5. 私たちは、サイバー領域がいわゆるサイバー戦や情報戦などの舞台となり、自衛を名目とした武力行使を含む戦争にも関与するものとなる法改正に反対する。

5.1. 「防衛戦略」における情報戦の記述

「防衛戦略」には以下の記述がある。

> 精密打撃能力が向上した弾道・巡航ミサイルによる大規模なミサイル攻撃、 偽旗作戦を始めとする情報戦を含むハイブリッド戦の展開、宇宙・サイ バー・電磁波の領域や無人アセットを用いた非対称的な攻撃、核保有国が公然と行う核兵器による威嚇ともとれる言動等を組み合わせた新しい 戦い方が顕在化している。こうした新しい戦い方に対応できるかどうか が、今後の防衛力を構築する上で大きな課題となっている。
>
> (中略)
>
> サイバー領域においては、諸外国や関係省庁及び民間事業者との連携により、平素から有事までのあらゆる段階において、情報収集及び共有を図るとともに、我が国全体としてのサイバー安全保障分野での対応能 力の強化を図ることが重要である。政府全体において、サイバー安全保障分野の政策が一元的に総合調整されていくことを踏まえ、防衛省・自 衛隊においては、自らのサイバーセキュリティのレベルを

> 高めつつ、関係省庁、重要インフラ事業者及び防衛産業との連携強化に資する取組を 推進することとする。

注目すべきなのは

- 偽旗作戦を始めとする情報戦を含むハイブリッド戦の展開
- 核兵器による威嚇ともとれる言動等を組み合わせた新しい 戦い方
- 諸外国や関係省庁及び民間事業者との連携により、平素から有事までのあらゆる段階において、情報収集及び共有を図る
- 政府全体でサイバー安全保障分野政策を一元的に総合調整する

といった表現だ。

5.2. 情報戦の問題

サイバー領域の「戦争」には、殺傷力のある武器を用いて銃弾や砲弾、爆弾が飛び交うような戦場のイメージとはほど遠いものが多くある。そのひとつが「情報戦」だ。

戦時下の情報戦では、サイバー領域が、国籍や人種、民族、宗教、ジェンダー、価値観など様々な違いを理由に、国家や支配的な集団が憎悪や偏見、差別を扇動し、結果として自国の暴力を正当化するための場となる。

(参考)危機の時代におけるパレスチナ人のデジタル権利の尊重をテック企業に求める 市民社会団体の呼びかけ https://www.jca.apc.org/jca-net/ja/node/295

安保防衛三文書における能動的サイバー防御の考え方は、自衛隊のいわゆる敵基地への先制攻撃と関連するだけにとどまらない。サイバー領域全体を巻き込んだ情報操作や、サイバー領域全体の網羅的な監視・取り締まりの強化、いわゆる「敵」のソフトターゲット(民間人や民間の建物など警備や監視が手薄で攻撃されやすい軍事目標)を狙うなどの行動が重要な役割になる。

6. サイバー領域の戦争への加担は、自衛隊に限らず、企業、研究機関、団体、一般の市民の動員も想定される

6.1. NATOのサイバー戦争軍事演習に参加する自衛隊、警察、総務省、民間企業

NATOのサイバー戦争のための軍事訓練、ロックド・シールズに毎年日本は正式に参加している。防衛省のプレスリリース。 https://www.mod.go.jp/j/press/news/2023/04/18d.html 「参加部隊等」として以下のように述べられている。

> （１）防衛省
> 内部部局、統合幕僚監部、陸上自衛隊システム通信団、海上自衛隊システム通信隊群、航空自衛隊作戦システム運用隊、航空自衛隊航空システム通信隊、自衛隊サイバー防衛隊
> （２）他府省等
> 内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）、総務省、警察庁、情報

処理推進機構（ＩＰＡ）、ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）、重要インフラ事業者等

6.2. 経団連の積極的な対応

経団連は4月に開催した「サイバー安全保障に関する意見交換会」の記事で次のように述べている。

> 「経団連として、当該組織の新設に向けた法制度整備の方向性や「能動的サイバー防御」のあり方など、政府の動向を注視することに加え、民間としていかに取り組むべきか実務的な検討を重ねていくことは、極めて重要な課題である。」

7. サイバー領域が戦争に巻き込まれるとき、従来の戦争で想定されている武器の他に、私たちのパソコンやスマホもまた「武器化」し、人々が容易にサイバー部隊に動員され、企業もまたサイバー領域での戦争行為に容易に加担することが可能になる

7.1. ウクライナの「サイバー軍」に世界中から「参戦」している

(NHK)“サイバー攻撃＝犯罪だが…”　ウクライナ「IT軍」の日本人 参戦の理由
https://www.nhk.jp/p/gendai/ts/R7Y6NGLJ6G/blog/bl/pkEldmVQ6R/bp/pM2ajWz5zZ/

ウクライナのサイバー軍 https://itarmy.com.ua/instruction/?lang=en

7.2. 反戦平和運動の側でも武器の認識はない？

陸上自衛隊システム防護隊初代隊長だった伊東寛は著書『サイバー戦争論』(原書房)で次のようにサイバー戦争の特徴について述べている。

> 「21世紀のサイバー戦争においては、戦線とか戦域といった物理的空間の境界や領域は存在せず、戦場はサイバー空間である。ここでは直接、敵の姿を視認することもなく、血をみることもない。そのような戦場では、これまで戦争に無関心、あるいはそれを避けていた人々も容易に戦争に参加できるのだ。攻撃対象は敵軍そのものでなくても良い。敵軍の兵站を支える物流システムであったり基礎となる通信網、あるいは敵国の経済システムそのものであったりしても構わない。」
> 「サイバー技術は、人々が否応なく巻き込まれる戦争から、人々が勝手に参加する戦争へと、戦争自体の性格を変えるものだと言える」(p.35)

パソコンのような私たちの誰もが所持したり自由に使える道具が、サイバー領域における軍事行動—諜報活動や情報戦からドローンにミサイル発射を指令するコマンドまで—では主要な武器になる。しかし、政府も法律も、これを武器としての定義には含めていない。反戦平和運動の側でも武器の認識はない。

実際はどうかといえば、パソコンはすでに実空間の戦場でも戦闘行為に必須の機器になっているが、サイバー領域では、これが主役の武器と化す。上述したロックド・シールズの軍事演習で用いられたコンピュータは、敵のシステムを攻撃し、敵からの攻撃を防御する武器だ。

8. サイバー領域を戦争に巻き込む体制が世界規模で急速に進行するなかで、私たちは、むしろサイバー領域をこれ以上戦争に加担させないための行動をとる必要がある。

8.1. 国連の警告

2021年6月29日、安全保障理事会でサイバー脅威に関する初の討論が行なわれ、軍縮担当上級代表の中満泉が「デジタル技術の「爆発的な」成長が紛争の新たな可能性を生み出している」とスピーチした。以下、国連のサイトから、この会合についてのレポート。

> 中満泉氏は、偽情報キャンペーンからコンピュータ・ネットワークの破壊に至るまで、近年、悪質な事件が劇的に増加しており、国家間の信頼と信用を低下させる一因となっていると指摘した。 特に危険にさらされているのは、金融機関、医療施設、エネルギー網など、情報通信技術（ICT）に大きく依存している重要インフラである。https://press.un.org/en/2021/sc14563.doc.htm

日本政府は、こうした警告や危惧があるにもかかわらず、むしろ率先してサイバー脅威を助長するような政策をとろうとしている。

9. サイバー領域はまさに、コミュニケーションの中枢を担う領域であるからこそ、この領域を戦争のために利用したり、戦争に巻き込んだりすることは絶対に許してはならない

むしろ私たちが希求すべきことは、サイバー領域における平和だ。サイバー領域から自衛隊を含む軍隊の活動を排除するだけではなく、民間企業や私たち一人一人がサイバー戦争に加担したり、強制されたりすることを徹底して禁じる必要がある。

サイバー領域の平和は、サイバー領域が文字通りの意味で、国境を越えて、多様な民衆を相互に繋ぐコミュニケーションの場となることでもある。この意味でも、サイバー領域における平和が今こそ求められている。

2021年のイスラエル軍によるガザ爆撃の後に、GoogleやAmazonの労働者からの呼びかけで立ち上げられたキャンペーン「アパルトヘイトのためのテクノロジーはいらない」は、Googleなどの巨大企業の労働者たちが、技術の軍事利用に反対して立ち上がった例だ。

> イスラエル軍がガザの住宅、診療所、学校を爆撃し、2021年5月にエルサレムのパレスチナ人家族を家から追い出すと脅しているとき、Amazonウェブサービスと Googleクラウドの幹部は、イスラエル政府と軍にクラウドテクノロジーを提供する12億2000万ドルの契約に署名した。イスラエルのアパルトヘイトと取引することで、AmazonとGoogleはイスラエル政府がパレスチナ人を監視し、彼らの土地から

強制的に追い出すことを容易にする。https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/notechforapartheid_jp/

10. 残念ながら日本政府の態度は、このサイバー平和とは真っ向から対立するものと言わざるをえない

岸田政権は、日本がサイバー戦争に踏み込むことを可能にするために、 障害となる憲法の保障する通信の秘密を形だけのものとしようと電気通信事業法、不正アクセス禁止法、ウイルス作成罪などを含む刑法、そして自衛隊法などの改悪を行おうとしている。

法律との関係では

- 現行法の解釈を国家安全保障に都合のよいように改める。
- 新規立法

このいずれも、国家安全保障を優先させる場合には、必ずといっていいほど私たちの基本的人権がないがしろにされることになる。

11. 通信の秘密、表現の自由は民主主義社会の基礎。能動的サイバー防御はこれを否定するものだ。

能動的サイバー防御が包括する範囲は、自衛隊の活動領域に加えて、私たちのコミュニケーションのほぼ全ての領域に関わる。私たちのコミュニケーションの領域に限ってみれば安全保障を口実として

- 通信の秘密が政府によって侵害される
- サイバー上の表現の自由が監視される
- SNSなどを利用した政府のプロパガンダに加担させられる

これら結果として、世論のなかに、敵意が醸成され、戦争を正当化する「空気」が形成されるとともに、社会のなかの思想信条であれエスニシティであれ、マイノリティフループが敵意の標的にされ、これを政府が後押しする。

サイバー領域は、私たちのコミュニケーションの領域でもある。つまり、思想信条や言論表現の自由を具体的に実現するためのインフラである。民主主義はこの自由権を前提にするときにのみまともに機能する。サイバー領域を安保体制に含めることは、サイバー領域に軍事基地が存在するようなもので、フェンスで交通が妨げられたり、人々の行動が監視される事態が常態化することを意味する。

12. サイバー領域の平和のために何をすべきか

伝統的な「戦争」の概念を根底から再考することが必要。もはや、戦場と銃後の区別はないし、人々の憎悪や偏見を煽るのはマスメディアや政府お抱えのメディアだけでなく、庶民が日常的に発信するSNSが有力な情報戦の武器になっている。

- サイバー領域を軍事安全保障から明確に切り離すこと
- 政府の非軍事部門は、国家のサイバーセキュリティなどを口実とした軍事安全保障に加担しないこと
- 民間企業は、サイバー領域における軍事安全保障に加担しないこと

_ サイバー戦争の武器は私たち自身がすでに持っているスマホやパソコンだったりする。このことを自覚しつつ情報戦に対抗するためには、社会の多くの人々が抱く偏見や差別、憎悪の感情を生み出す構造に目をむけることも必要になる。

- 情報通信のネットワークの技術的構造そのものに軍事的な利用や基本的人権を侵害するような利用を排除するような仕組みを組込むこと。
- IT企業の労働者が平和に反するような企業の活動に協力しないような運動を構築すること。

現在の陸海空の軍事力はコンピュータテクノロジーやサイバー領域と不可分であり、根本的にはこうした従来の武力そのもの放棄することが必須となる。そのためには「専守防衛」といったあいまいな文言で自衛隊を容認することはできない。暴力(武力であれ自衛力であれ何であれ)という手段をとらない政治なくしてサイバー領域の平和もなく、サイバー領域の平和がなければ、国境を越えた人々の連帯と信頼のコミュニケーションもありえない。

Author: 小倉利丸
Created: 2023-10-17 火 21:50
Validate