# サイバー安全保障「提言」批判


## 小倉利丸

最新および注の URL へのアクセスには右の QR コードで私のブログにアクセスしてください。
https://www.alt-movements.org/no_more_capitalism/blog/2025/01/22/cyber-anpo_teigen_hihan/


## Table of Contents



## 1. はじめに

能動的サイバー防御を可能にする法整備が、2025 年の通常国会で審議されることになる。能動的サイバー防御という言葉は、安保・防衛 3 文書[1]のなかで始めて登場する。この能動的サイバー防御は、官民一体で敵基地攻撃能力を合法化して先制攻撃を可能にする戦争体制のなかのサイバー領域における軍事行動の合法化を目指す枠組であり、すでに成立している経済安全保障の枠組とも連動することになる。また、より幅広い総動員体制を視野に入れれば、マイナンバー制度による人口監視との連動も将来的にはありうると考えてよいだろう。

本稿では、能動的サイバー防御を可能にする法整備のための有識者会議が昨年 11 月に出した「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」(以下「提言」と略記)[2]を対象にして、その問題点を洗い出し、サイバー領域を戦場にしないことを、戦争放棄の観点から検討する。同時に、サイバー攻撃と呼ばれる事象に特徴的なこととして、この「攻撃」が軍事安全保障に限定されず、より広範にはサイバー犯罪として警察が取り締まりの対象にしてきた事案をも包摂することがいかなる深刻な問題を引き起すかについても検討する。このことは、従来の武力の行使と威嚇という意味での「戦争」という観点で「提言」を解釈することでは十分ではないことを意味している。刑事犯罪領域を「提言」は国家安全保障に繰り込む視点をとっており、結果として、警察の活動もまた軍事・国家安全保障の枠組に包摂されるものとされている。しかも、先制的な敵基地攻撃能力同様に、能動的サイバー防御も先制攻撃を想定しており、全体として、未だ具体的な紛争や抗争が生じていない段階で国家が暴力装置を発

1 https://www.cas.go.jp/jp/siryou/221216anzenhoshou.html
2 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、https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html。 提言は https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf

動すべき、という考え方をとることになっている。そのために、警察については、治安維持を目的とした予防的な強制力の行使を可能にするような制度の転換が図られることになる。この傾向は、テロ対策同様、警察と自衛隊を横断し、国内と国外をも跨る形で対処の枠組が国家体制全体を覆うような規模へと大きく舵を切るものだと考えている。こうした点を踏まえて、戦争という概念を、自衛隊や警察が組織的に「力 force の行使や威嚇」を行うものと幅広く定義しておきたい。[3]私は、サイバー領域における「戦争」は、刑事司法の領域をも包摂しつつ、その舞台が情報通信のネットワークという非常に理解しづらい技術的な場で展開されているものであるという点で、従来型の戦争の枠組を前提にイメージして論じたり批判するだけでは、その危険性や問題を十分には捉えきれない特異な性格をもっている、とも考えている。

「提言」の枠組は、安保・防衛 3 文書で述べられているサイバー領域の軍事安全保障の考え方を新たな法制化へ向けて整理したもので、今後国会に提出される法案の基本的な考え方を示すものだ。「提言」の位置づけは「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ための新たな取組の実現のために必要となる法制度の整備」としているから、憲法 9 条の規定は最初から無視されている。その上で、官民連携の強化、通信情報の利用、アクセス・無害化、という三つの課題を軸に法整備のための基本を呈示した。議論の争点は幾つもあるが、そのうち通信への網羅的な監視や情報収集、令状主義を形骸化して犯罪捜査よりも治安維持目的での警察力の監視活動を合法化する法整備に関する箇所は、メディアも注目し繰り返し批判的な記事や論評も出されているので、逐一の批判は省き、二点だけ私の考え方を述べるにとどめる。[4]

## 2. 「提言」の盗聴あるいは情報収集について

「提言」では、「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」として、盗聴捜査に限らず情報通信への詳細で十分な情報収集を可能にすることを求めている。アクセス・無害化を念頭に置いているので、こうした取り組みは警察など盗聴法が盗聴を認めている捜査機関だけでなく自衛隊などもその主体として想定されている。従来の通信への捜査機関などによる盗聴では事件が起きた後で実施されるのに対して、提言が目指す通信情報の利用はこれとは本質的に異なるものだとして、以下のように書かれている。

> 今般実現されるべき通信情報の利用は、重大なサイバー攻撃による被害を未然に防ぐため、また、被害が生じようとしている場合に即時に対応するため、具体的な攻撃が顕在化する前、すなわち前提となる犯罪事実がない段階から行われる必要がある

従って、単に盗聴法の対象犯罪などを拡大するというだけでは済まされない。つまり

- 事案の発生前から監視を網羅的に実施できるようにする
- 警察だけでなく自衛隊もまたこうした権限を付与される

3 ここでいう「力」とは force を意味する。force は「武力」とも訳すことができる。
4 朝日新聞社説：サイバー防衛⬚厳格な歯止めの議論を 2024 年 8 月 24 日、https://www.asahi.com/articles/DA3S16017418.html 毎日新聞社説、能動的サイバー防御⬚国民の権利を侵さぬよう https://mainichi.jp/articles/20240611/ddm/005/070/088000c、 信濃毎日新聞社説 サイバー防御⬚厳格な歯止めが不可欠だ https://www.shinmai.co.jp/news/article/CNTS2025011200013、 市民団体などの反対声明として下記がある。秘密保護法対策弁護団、【声明】通信の秘密を侵害する能動的サイバー防御制度の導入に反対する声明 https://nohimituho.exblog.jp/34227610/ (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の平和を https://www.jca.apc.org/jca-net/ja/node/296

ということが必要要件となる。「提言」では、大胆にも「これまで我が国では存在しない新たな制度による通信情報の利用が必要」だと述べている。

「提言」では通信情報の分析は、問題を未然に防ぐ予防手段であるため、既遂の行為について真実を解明することを目的とする犯罪捜査とは動機も目的も異なる。「提言」はこの点を次にように強調している。

> 通信情報を取得しようとする時点では、いかなる具体的態様でサイバー攻撃が発生するかを予測することはできず、あらかじめそのサイバー攻撃に関係する通信手段、内容等を特定することは通常は困難であるから、犯罪捜査とは異なる形で通信情報を取得し利用する必要があり、被害の防止と通信の秘密の保護という両方の目的を適切に果たすためには、これまで我が国では存在しない新たな制度による通信情報の利用が必要である。

上の立場はこれまで政府の見解を真っ向から否定するものでもある。これまで政府は、捜査機関の盗聴が憲法 21 条の「通信の秘密」に抵触しない理由を以下のように解説している。[5]

> 通信傍受は，捜索・差押えと同じように，具体的な犯罪行為が行われた場合に，これに関連する捜査として行うものです。何か犯罪が起きるかもしれないということで通信の傍受を行うことはできません。
>
> また，特定の個人や団体がどのような活動をしているかを探るなど，いわゆる情報の収集のために行うものではありません。

盗聴捜査は「具体的な犯罪行為が行われた場合」であって「何か犯罪が起きるかもしれないということで通信の傍受を行うことはできません」と明言している。「提言」は逆に、「何か犯罪が起きるかもしれないということで通信の傍受を行うこと」が必須だ、としており、従来の政府見解が示していた通信傍受の合憲性の主張の前提を根底から否定するものだ。だから「これまで我が国では存在しない新たな制度」が必要だというのだ。しかもこのような立場は、自民党の改憲草案ですらとっておらず、自民党改憲案をも越えている。

## 3．憲法 21 条と「公共の福祉」

その上で憲法 21 条 2 項の通信の秘密条項については「通信の秘密であっても、法律により公共の福祉のために必要かつ合理的な制限を受けることが認められている」とし、公共の福祉を理由に予防的な通信傍受が可能だ主張している。公共の福祉を理由に通信の秘密の権利を制限するという政府の態度はこの間一貫している。

たしかに憲法 12 条には、「この憲法が国民に保障する自由及び権利は、国民の不断の努力によつて、これを保持しなければならない。又、国民は、これを濫用してはならないのであつて、常に公共の福祉のためにこれを利用する責任を負ふ」とあり、13 条以下の条文はこの 12 条の「公共の福祉」という縛りを前提にしていると読むことが可能ではある。しかし、私はこの解釈をとらない。というのも、22 条、29 条では改めて「公共の福祉」が明記されており、明記されている条文と明記がない条文という違いがなぜ存在するのかという点に注目すべきだと考えるからだ。

私は、一般に言論表現の自由(通信、学問、宗教などの自由)に憲法では「公共の福祉」を明記していないのには理由があると考えている。もし自由の権利に「公共の福祉」という制約を課すことになると、「公共」の解釈いかんでは、国家や社会の支配的な価値観の優位性を認めることになりかねない。特に日本では「公共」を口実とし

5 https://www.moj.go.jp/houan1/houan_soshikiho_qanda_qanda.html 最高裁判例も参照。
https://www.courts.go.jp/app/files/hanrei_jp/400/050400_hanrei.pdf

て国益を優先させて個人の自由を制約しようとする対応がある。こうした日本の現実をみたとき、21 条の通信の秘密に「公共の福祉」を読み込むと、実際の表現行為、通信内容、学問への国家の監視を正当化しかねない。あるいは親密な恋人同士がプライベートなやりとりのなかで、公然化されれば猥褻とみなされるようなデータのやりとりを通信することもありえるが、こうした通信を「公共の福祉」を口実に規制するために監視するといった権力によるプライバシーへの過剰な介入も予想できる。だから、各条文で「公共の福祉」を明示していないものについては、「公共の福祉」という制約を課すことのない権利として、つまり、時としては公共の福祉を逸脱しても構わないような表現や通信、学問、宗教が存在する余地があると解釈する必要があると考えている。[6]

「提言」が主張は、通信の秘密に「公共の福祉に反しない限り」という制約を課すことによって、サイバー領域における「戦争」に連動する情報通信の活動が行なわれていないかどうかを網羅的に監視できる法制度の導入を許すことになることから、通信の秘密全体を否定することになり、こうした解釈は絶対に認めてはならない。

言うまでもないが、「公共の福祉」という解釈の立場をとれば、未だ起きていない事案を事前に監視し取り締まるような権力行使が認められることにはならないことも付言しておく。

## 4．通信の秘密は国外に及ぶのだろうか

「提言」が対象としているのは犯罪から戦争あるいは武力紛争に関するサイバー領域に至るまで広範囲にであり、全体の枠組は、国内向けの対応では警察が主体になり、対外的な武力行使関連対応では自衛隊が主体になる、という役割分担が考えられていると思われる。[7] この全体の枠組のなかで通信の秘密という私たちの権利を考えなければならないが、同時に情報通信の基盤がグローバルなインターネットによって支えられ、「私たち」という言葉には私たちが繋りあっている世界中の人々とのコミュニケーションが含まれることを自覚的に認識しておく必要がある。

このこと前提にして、憲法が権利として定めている通信の秘密は、日本国内の日本の「国民」にのみ適用される権利ではなく、それ以外の人々に対しても日本政府は通信の秘密を守る義務を負うものと解釈すべきである。つまり、日本は世界中の誰に対しても通信の秘密を侵害するような権力の行使を行うことは憲法で禁止している、ということだ。もし、通信の秘密が「日本国民」のみに与えられた権利であるとすると、外国の主権の問題はともかくとして、日本の政府機関が外国において盗聴活動を行なうことを日本の憲法は禁じていない、ということになる。従来であれば、国外での盗聴捜査は、警察などであれば捜査共助条約などを通じて相手国の捜査機関に依頼するなどになる。しかし、犯罪の実態がなく情報収集を目的に盗聴活動を行なう場合は、この仕組みも使えない。自衛隊の場合も同様に、国外での情報収集の権限の是非についての明文規定はない。しかし、「提言」の趣旨を制度化するとなると、外国の主権が及ぶサイバー領域において、その主権を侵害しても日本の国益を優先させて情報収集活動を行うことも視野に入れた法制度になる可能性がある。つまり、スノーデンが日本でやっていたような諜報活動のようなことを日本がやれるようにしたい、ということが想定されている。自衛隊や他の政府機関がスノーデンのような活動を行うこと

6 実は現行憲法で公共の福祉を明記していない条文について、自民党の改憲草案では、これを明記する方向での改正を提案している。 https://storage2.jimin.jp/pdf/news/policy/130250_1.pdf つまり自民党は現行憲法の「公共の福祉」が明記されていない条文については、公共の福祉を逸脱する場合も憲法が私たちの権利を保障していると解釈される余地があることを危惧している。私はヘイトスピーチのような言論を全く支持していない。ヘイトスピーチは差別を肯定する言論であり、社会的な平等に基づく人々の自由の権利と真っ向から対立する。これは公共の福祉の問題ではなく、構造的な差別の問題である。

7 傍受令状の請求可能なのは、検察官、司法警察員、麻薬取締官及び海上保安官だけである。犯罪捜査のための通信傍受に関する法律第４条。https://laws.e-gov.go.jp/law/411AC0000000137

ができる法的制度的な枠組は現在では存在しない。今後の政府の方向は、自衛隊など軍事安全保障に関わる組織が国外で諜報活動を行うことを合法化する制度の整備へと向かう可能性がある。これが提言が強調する安全保障の力を「欧米主要国と同等以上に向上」させる、ということに含意されていることのひとつだろう。

以上の点を踏まえて、強調したいことは、通信情報の世界はシームレスに世界を繋いでおり、インターネットのシステムは世界でひとつの構造をもっているという状況で、情報が国境を越えて流通する中で、日本がサイバー攻撃を受け、あるいはサイバー攻撃の主体となるような事態のなかで、私たちは、自分たちの情報通信環境に関連する通信の秘密、言論表現の自由、結社の自由、思想信条の自由といった市民的自由の原則を守るためのより強固で断固とした闘いを組む必要がある、ということだ。市民的な自由の観点からみたとき、国境を越える通信は、日本国内だけでなく国外の人々と私たちの通信の秘密の防御は必須であり、同時に市民的な自由がグローバルな人々の権利の平等を前提とするならば、通信の秘密は差別なくすべての人々に保障されるべき権利である。このことを前提として、また国際法の原則も踏まえて[8]、日本政府が国外において、あるいは日本国民以外の人々にも通信の秘密の権利を保障するような基本的な姿勢をとることが憲法上の義務でもある、と考えるべきだろう。とりわけ戦争・武力紛争において、市民の運動としては、日本政府が敵国とみなす国の人々に対しても平等にその権利を保障すべき、という観点を明確にした取り組みをすることが重要なことだ。たとえば、外国にあっても、人々が自国政府からの通信への厳しい監視があるという場合、日本政府はこうした人々の通信の秘密の権利を保障する立場をとるべきであり、また、日本国内に暮す外国籍の人たちにも平等に保障されるべきである。

## 5. 「サイバー戦争」の四つのケース

サイバー領域の「戦争」は、実空間の戦争あるいは戦闘行為とはその範囲も国家、社会の諸制度の関わり方も大きく異なる。サイバー領域の戦争には大きく分けて四つのケースがある。

### *5.1. サイバー領域で完結する場合*

サイバー領域が「戦場」を構成する場合で、その影響がサイバー領域に留まる場合もあれば、結果として実空間における施設や組織、あるいは人間に対して打撃となる場合もある。

この場合にも二つの主要なケースがある。ひとつは、情報通信ネットワーク上を監視して情報を収集し、将来の攻撃の準備をする場合。ネット上のスパイ活動である。もうひとつのケースは、ネットワークを介して重要な社会インフラの機能をマヒさせるなどの攻撃を行なう場合であるが、ハッキングであれ無害化であれ攻撃の手段はサイバー領域を通じたものになり、おおむねサイバー領域で攻撃が完結する場合だ。「提言」が主に対象としているのはこのケースだ。したがって民間の通信事業者などとの連携を強化が強調されるとともに、政府の組織体制も明確に指揮命令系統が一本化されるような再編が必要だとされている。情報通信のネットワークは国家の中枢から経済基盤、私たちの日常生活を覆うので、官民を巻き込むの総力戦体制の構築になる。

「提言」では「アクセス・無害化」という表現を一貫して用いており、このサイバー攻撃にはアクセスに関わるが無害化には至らないケースが含まれている。無害化の場

8 「すべての者は、表現の自由についての権利を有する。この権利には、口頭、手書き若しくは印刷、芸術の形態又は自ら選択する他の方法により、国境とのかかわりなく、あらゆる種類の情報及び考えを求め、受け及び伝える自由を含む。 」国連、市民的及び政治的権利に関する国際規約（自由権規約）条約本文 https://www.nichibenren.or.jp/activity/international/library/human_rights/liberty_convention.html

合がかなり過激なシステムダウンなどの印象があるためにメディアなどの注目が集まりやすいが、「アクセス」はそれに比べて見逃されがちだ。しかしアクセス攻撃は、より広範囲で、かつその行動も露呈されにくいものであって決して無視すべきではない。「提言」が想定している「アクセス」は、私たちがウエッブにアクアスして情報を取得する、といった合法的なアクセスではなく、むしろ、日本国内の現行法では違法とされるいわゆる不正アクセスを合法化し、同時に、国外にあるネットワークなどに対しても、相手国あるいは国際法上からも違法とされるアクセスを実施できるようにするということが想定されていると思われる。つまり、政府機関によるハッキング行為の合法化である。

「提言」では「アクセス」と呼ばれているハッキングには様々な動機がある。近い将来無害化攻撃をすることを前提に行なわれる場合もあるだろうが、網羅的に情報を収集すること自体を目的とする場合もありうる。ビッグデータを AI を駆使して迅速に解析できる現代の技術水準を前提とすると、後者のようなハッキングがより重視されるかもしれない。いわゆる一方的に情報を収集するだけで実空間の社会経済基盤を物理的に機能不全に陥れることに直接直ちにはつながらない場合であっても、こうした収集データが将来において実空間での物理的な破壊攻撃(キネティック攻撃[9])の前提情報となりうるからだ。「アクセス・無害化」といっても、どのようにして情報を収集するのか、収集した情報を何を目的に利用するのかなどについては答えは一つにはならないのだ。

ちなみに、ハッキングの攻撃が開始されてから発覚するまでの平均日数は、日本の民間機関の 2022 年の調査では 397 日という結果もでている。[10]少し前、2015 年にセキュリティ・インシデント対応企業 Mandiant が発表したレポートでは侵害の最も早い兆候から侵害が発見されるまでの平均経過日数は 205 日、最長の経過日数 2,982 日とある。[11] また 2023 年に発覚したボルト・タイフーンの場合は潜伏期間が 5 年にもなると報じられた。[12]不正侵入を感知するための対策とハッキング技術の高度化のいたちごっこの状態で、発覚までの時間は決して短くはなっていない。

日本が「アクセス」を試みるという場合も、上記の事例のような長期の潜伏が重要な「アクセス」の目的のひとつになることは間違いない。攻撃の事案が起きる前に行動することになるので、長期の侵入を意図することになる。たぶん、長期のハッキング=スパイ行為を様々なところで行いながら、情報収集と解析を繰り返しつつ無害化の標的が選ばれるのだろう。このように考えると、無害化よりも「アクセス」の方がより深刻な通信の秘密やプライバシーの権利への侵害行為になる可能性がある。

同時に、無害化の実行については「提言」では以下のように述べている。

> 権限の執行主体は、現に組織統制、教育制度等を備え、サイバー脅威への対処に関する権限執行や武力攻撃事態等への備えを行っている、警察や防衛省・自衛隊とし、その保有する能力・機能を十全に活用すべき(である)

自衛隊や警察が関与の中心を担うべきだとしているが、自衛隊には国内での法執行権限がないので、対外的な対応の主体となり、警察はその捜査権限を用いて国内におけるサイバー攻撃への対応を担う、という役割分担を考えているのだろう。言うまでもなく、主体が自衛隊なのか警察なのかはどうでもいい問題ではない。戦争や武力紛争

9 「Kinetic warfare は、外交のような「ソフト」な力とは対照的に、軍事 戦闘やその他の直接破壊的な戦争形態を指す言葉。法律戦 lawfare、制裁、サイバー戦、心理戦、情報戦その他のタイプの「ソフト」な力と対照的である。この用語は、2000 年代に入ってから広く使われるようになる前に、軍事用語として登場した。」wikipedia https://en.wikipedia.org/wiki/Kinetic_warfare

10 https://www.cscloud.co.jp/news/press/202402216761/

11 https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1135998/active-defense-security-operations-evolved/

12 (Gigazine)中国政府系ハッカー集団「ボルト・タイフーン」が 5 年間以上もアメリカの主要インフラに潜伏していたことが判明、台湾侵攻の緊張が高まる https://gigazine.net/news/20240208-china-volt-typhoon-infrastructure-5-years/

に軍が関与するだけでなく警察が関与して敵のサイバー領域を攻撃するとなると、果して、これが現行法の「警察」活動の枠組に入れうるのだろうか。そもそも警察法2条の「警察の責務」は「犯罪」に関する事案であり戦争や武力紛争ではない。しかし、テロ対策の前例がある。テロが刑事事件のカテゴリーから米国の対テロ戦争をきっかけに、国家安全保障の主要課題に格上げされながらも警察は依然としてテロ対策を重要な活動の柱としてきた。こうして警察は刑事警察からより治安維持へと軸足を移すきっけをつかんだ。今回はより広範囲に戦争全体を網羅する形で警察が軍事安全保障に関与することになる。しかも「提言」では以下のように述べている。

> 新たな制度の目的が、被害の未然防止・拡大防止であることを踏まえると、インシデントが起こってから令状を取得し、捜査を行う刑事手続では十全な対処ができないと考えられ、新たな権限執行には、緊急性を意識し、事象や状況の変化に臨機応変に対処可能な制度とする必要がある

令状によらない強制捜査や事件の発生がない段階での予防的な治安維持のための警察権力の権限強化が確実に伴うことになる。令状主義の形骸化は、国連のサイバー犯罪条約においても強調されているから、今後、こうした方向は確実に強まると警戒する必要がある。

## *5.2. 情報戦*

「提言」では情報戦についてのまとまった記述はない。安全保障戦略では「領域をめぐるグレーゾーン事態、民間の重要インフラ等への国境を越えたサイバー攻撃、偽情報の拡散等を通じた情報戦等が恒常的に生起し、有事と平時の境目はますます曖昧になってきている」とし「武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性が高い」としていた。そして「偽情報等の拡散を含め、認知領域における情報戦への対応能力を強化する」こと「外国による偽情報等に関する情報の集約・分析、対外発信の強化、政府外の機関との連携の強化等のための新たな体制を政府内に整備する」と明言していた。

「提言」には情報戦も偽情報も登場しない。たぶん、この課題は別途追求されることは間違いない。多分政府は、このプロパガンダや偽情報といった意味での情報戦領域は、あえて法整備が必要とはいえず現行法で対応可能なものだと判断しているのかもしれない。

一言強調しておきたいのだが、外国が偽情報の拡散を行うという認識は、これに対抗して日本もまた偽情報の拡散を行うであろう、ということも含意していることに私たちは注意する必要がある。しかし、日本政府が発信する偽情報について日本の現行法には何の規制も制約も課していない。むしろ政府による偽情報を規制する制度が必要だろう。

これに対して「提言」で言及されていない「サイバー戦争」の重要な領域があと二つある。

## *5.3. 自衛隊の陸海空などの戦力と直接連動したサイバー領域。*

兵器や装備を実際に使用するためには標的の把握などでコンピュータのネットワークや AI による情報処理は必須の条件になる。実際の戦争のためには、標的の確認が必要になる。標的が人間の場合は、移動を把握しなければならない。相手国のデータは多ければ多いほどよく、この意味で情報収集は必然的に網羅的になる。この領域は自衛隊の組織内部で対応できる領域であり新たな法制化なしに――自衛隊の組織再編では何らかの法制度の対応が必要だろうが――対処できる領域だと判断し「提言」は言及していないのかもしれない。

このケースに該当する「戦争」として実際に行なわれてるものとしては、現在も進行中のイスラエルのガザ戦争がある。イスラエルはガザの住民に関する膨大な人口や住宅などの地理データを保有している。これらとリアルタイムでの人々の移動を通信やドローンなどで監視し、攻撃対象を特定して空爆などを実施している。こうしたシステムには、米国の Google や Amazon も技術やクラウド・サービスで協力している。[13]

### *5.4. 無害化攻撃が実空間における武力行使のための露払いとなる場合*

ハッキングやサイバー攻撃といった「アクセス・無害化」が実空間における武力行使のための露払いとなる場合がある。たとえば、相手の軍事施設のネットワークや社会インフラを無害化した後で武力行使へ転ずる、といった使い方がありうる。しかし「提言」ではこの領域に関連する法整備には言及がない。

サイバー領域での長期にわたるスパイ活動や無害化攻撃を遂行した後に、自衛隊の実力部隊が実空間での武力による破壊攻撃活動を展開する、という流れは現在の戦争・武力紛争のひとつのタイプになりつつあるように思う。たとえば、安保戦略で議論になった敵基地攻撃に先行して、情報収集や敵の軍事関連のインフラなどへのサイバー攻撃を仕掛けて反撃能力を削いだ上で敵基地や重要インフラへの攻撃を実行する、という流れが考えられる。脅威圏の外から敵に対処する「スタンドオフ」という考え方が強調されていることからも、こうしたサイバー領域を効率的に活用して実空間での攻撃のリスクを最小化することが当然考えられる。

こうしたケースで日本が戦争に関与する場合、米国などいわゆる同盟国との連携が重要になりそうだ。たとえば、サイバー領域における先制攻撃を日本が担い、実空間での攻撃を他の同盟国が担う、という役割分担は現在の日本の法制度からすると取り組みやすいかもしれない。現行法では外国の軍隊のようには自由に動員できない自衛隊の制約があり、政府は、改憲を通じて自衛隊が軍隊としての体制を整え、軍事組織関連の法整備が整うことが先決と考えているのかもしれない。事実 NATO のサイバー演習「ロックドシールズ[14]」に日本から自衛隊だけでなく情報通信関連の省庁や民間企業も毎年参加して他の NATO 加盟国などとタッグを組んでのサイバー攻撃への取り組みを行なっている。

## 6. 無害化攻撃と攻撃元の特定問題

ここでは、敵とみなされたシステムのアクセス・無害化を中心に「提言」の問題点を指摘したい。アクセス・無害化攻撃が必要とされる前提にある現状認識について「提言」は以下のように述べている。

> 近年、サイバー攻撃は巧妙化・高度化している。具体的には、サイバー攻撃は、複雑化するネットワークにおいて、国内外のサーバ等を多数・多段的に組み合わせ、サーバ等の相互関係・攻撃元を隠匿しつつ敢行されている。また、ゼロデイ脆弱性の活用等により、高度な侵入が行われるほか、侵入後も高度な潜伏能力により検知を回避するなど、高度化している。このため、サイバー攻撃の特徴としては、現実空間における危険とは質的に異なり、実際にある危険が潜在化し認知しにくいということが挙げられる。また、潜伏の高度化等により、攻撃者の意図次第でいつでもサイバー攻撃

13 たとえば以下を参照。(+972magazine)「ラベンダー」： イスラエル軍のガザ空爆を指揮する AI マシン https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/972magazine_lavender-ai-israeli-army-gaza_jp/ (+972Magazine)「大量殺戮工場」： イスラエルの計算されたガザ空爆の内幕 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/972magazine_mass-assassination-factory-israel-calculated-bombing-gaza_jp/、

14 防衛省「ＮＡＴＯサイバー防衛協力センターによるサイバー防衛演習「ロックド・シールズ２０２４」への参加について」https://www.mod.go.jp/j/press/news/2024/04/23c.html

> が実行可能であるとともに、ネットワーク化の進展により、一旦攻撃が行われれば、被害が瞬時かつ広範に及ぶおそれがある。

上の引用にあるように、サイバー攻撃は「サーバ等の相互関係・攻撃元を隠匿しつつ敢行されている」のが通常のありかたになる。一般に実空間での武力行使では、武力による優位を相手に自覚させて相手の更なる攻撃を抑止しようとする動機があり、攻撃の主体であることを隠さない場合が一般的だろう。これに対してサイバー領域では、逆に、サイバー攻撃の事実があり被害もあるとしても、この攻撃の責任の帰属先が意図的に隠蔽され、また攻撃後も名乗り出ない、ということが少くない。

たとえば、サイバー攻撃の非常に早い時期の典型事例として挙げられるのが、米国のオバマ政権の時代、2011 年頃から開始されたイランの核濃縮施設への極秘のサイバー攻撃(コードネーム Olympic Games)がある。この攻撃は米国とイスラエルが共同で開発した Stuxnet と呼ばれるコンピュータプログラム(ワーム)を密かにイランの核施設に送り込みシステムを機能不全に陥らせた。[15] このケースはニューヨークタイムズがすっぱ抜いたために明るみに出たが極秘の作戦であリ、現在も米国政府は自らの攻撃だとは認めていない。

攻撃元が誰なのかを特定して攻撃の責任の帰属を明確にすることは戦争における責任問題として重要である。この攻撃元の帰属を「アトリビューション」と呼ぶ。「攻撃者サーバ等へのアクセス・無害化」と「提言」は簡単に言うが、実際には誰に責任があるのかを証明するのは容易ではない難問であり、このことアトリビューションの妥当性自体が国際的な紛争の主題にもなる。この点への「提言」の言及は十分とはいえない。しかも「提言」の目的は、武力攻撃事態に至らない状況において、某国の何らかのシステムが将来の攻撃者であると特定して先制攻撃を仕掛けることになる。アトリビューションを予断や陰謀ではなく、第三者にも納得できる証拠によって果して証明できるのだろうか。つまり、無害化攻撃の標的となる「攻撃者」に関するアトリビューションをどう考えるのかが「提言」ではあまりにも軽く扱かわれている。

アトリビューションが重要なのは、一般に、国際紛争を武力行使によって解決するという方法は禁じられており、例外が自衛権の行使になり、正当な自衛権行使であることを主張するためには、攻撃者を客観的な証拠に基いて特定し、第三者からもその証拠の妥当性が得られることが重要になるからだ。攻撃された側が独断で「あいつがやった」と攻撃元を名指ししたとしても国際的な理解が得られなければ孤立するかもしれない。未だに攻撃がない段階で先制的なサイバー攻撃を行使するとなると、このアトリビューション問題は飛躍的に難度が高くなるだろう。しかも、アトリビューションの根拠情報は、自国の機密に属するような諜報活動や、もしかすると違法とされるような情報収集活動あるいは同盟国からの秘密裡での情報提供など、いずれも公開しがたい情報である場合が多いとみていい。

## 7．日本が攻撃元であることは秘匿されるに違いない――独立機関による事前承認などありえない

サイバー攻撃は、平時においても採用できる軍事攻撃である。上記のアトリビューションの困難さも考慮したとき、日本が「アクセス・無害化」攻撃を名乗りを上げて行うだろうか？むしろ密かに、日本が攻撃元であることを秘匿して実行するはずだ。そして、実行元を秘匿する攻撃こそがサイバー攻撃の一般的な姿でもある。ところが『読売新聞』は、先制的なサイバー攻撃を実施する場合の手続きについて以下のように報じている。

> 撃元サーバーへの侵入・無害化措置は、通信情報の分析で重大なサイバー

15 https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

> 攻撃の恐れがあると判明すれば、警察・自衛隊が実施する。事前承認する独立機関は、公正取引委員会などと同様に独立性の高い「３条委員会」に位置づけ、内閣府の外局とする方向だ。[16]

攻撃事前承認が必要で、しかもこれを独立機関に担わせる、という。私は、攻撃は極秘であることが大前提になるから、このような手続きはありえないと思う。しかも、たとえ第三者委員会のようなものを設置してもアトリビューションの実質を確保できるだけの機密情報が開示されるはずもない。とりわけ同盟国などから提供された情報であればなおさらだろう立法過程で野党を黙らせる手段として提起されただけのものだ。しかも、更に悪いことには、第三者委員会の承認は、一般世論に対して、あたかも客観的で攻撃の妥当性が証明されたかのような印象を与える効果を生むことになる。

従って、サイバー領域における日本の「アクセス・無害化」攻撃は、公式には公表されず隠蔽され、公表されることはまずありえない、と考えるべきだ。このことは、日本の軍事・安全保障領域に極めて大きなブラックボックスが構築されることを意味している。法律が成立した後でも、敵国からのサイバー攻撃の報道は頻繁にあるだろうが、日本からのサイバー攻撃などの動きが迅速に報じられることは極めて少ないだろう。しかし実際には日本が水面下で長期戦を覚悟でサイバー攻撃を仕掛けているはずであって、私たちに知らされないなかで、戦争の危機が深化するという事態になる。

こうした事態を回避する唯一の方法は、独立委員会とか第三者委員会を設置して歯止めにするといった見当違いな対応ではなく、サイバー攻撃という手段をとることができないような制度的な枠組を構築し、同時に、サイバー領域を戦争に巻き込むあらゆる兆候を排除するということを徹底することにある。そのためには日本であれ諸外国であれ、攻撃の動機そのものをもたないような国際関係の構築を目指すことこそが最良の手段だろう。

## 8．アクセス・無害化攻撃と民間の役割

アクセス・無害化攻撃は警察や自衛隊が実施するとされているが、果してその準備から実行までの全過程を民間の通信事業者の協力なしで実施することができるだろうか。ネットワークの動向を現場で最初に把握できるのは実際にサーバーやネットワークを運用している事業者だ。最近米国を中心に起こされたボルトタイフーンと呼ばれるサイバー攻撃の最初の発見者でありアトリビューションにも重要な貢献をしたのはマイクロソフト社だった。[17]

通信事業者が戦争に加担しない限りサイバー領域を巻き込んだ戦争は不可能である。こうなると、武力行使の主体は自衛隊や警察に限定されないことになる。そうなれば、当然相手国の反撃の対象も「民」を巻き込むことになる。それだけではなく、こうしたサイバー戦争の主体に一部に民間が関与した場合、当然民間であっても相手国は力の行使主体とみなして、攻撃の対象とすることも考えられる。もちろん日本が攻撃主体になるときも、同様に正当な攻撃の標的に相手国の民間の通信事業者が含まれることになる。

政府のサイバー攻撃を「民」が一部担うようなケースの場合について、NATO のサイ

16 2025 年 1 月 15 日。 https://www.yomiuri.co.jp/politics/20250114-OYT1T50191/

17 「Microsoft は、標的を絞った悪意あるステルス活動を発見しました。米国内のさまざまな重要インフラストラクチャ組織を狙い、侵害後に資格情報アクセスとネットワーク システム検出を実行することを目的とした攻撃です。」 https://www.microsoft.com/ja-jp/security/security-insider/emerging-threats/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques ただし中国は攻撃元であることを否定し反論している。中国の反論は Volt Typhoon：A Conspiratorial Swindling Campaign targets with U.S. Congress and Taxpayers conducted by U.S. Intelligence Community https://www.cverc.org.cn/head/zhaiyao/futetaifengEN.pdf

バー戦争に関するルールブックともいえるタリン・マニュアル(バージョン2)[18]は以下のような解釈を示している。

> 国家機関の行為に加えて、国家機関として認められない個人または団体が、国内法（例えば、立法、行政行為、または国内法で規定されている場合は契約）によって政府当局の権限の一部を行使する権限を与えられている場合、 その行為は国家に帰属する。ただし、個人または団体が特定の事例においてその権限を行使している場合に限る。例としては、政府から他国に対する攻撃的サイバー作戦の実施を法的に認められた民間企業や、サイバー情報収集を法的に認められた民間団体が挙げられる。p.89

「提言」ではこうした民間企業による戦争への加担、時には戦争犯罪にすらなりうるリスクについて明示せず、関心をもっているとはいえない。しかもサイバー戦争への加担は、実空間での戦争とはちがって、リモートからパソコンなどを用いて容易に「参戦」することができる。事実ウクライナのIT軍は世界中からITの専門的な知識をもつ人材だけでなく、ほとんど専門の知識なしにインストールしたソフトウェアを使って攻撃に参加できる仕組みを作りあげてボランティアを募りサイバー攻撃の体制を構築している。[19]日本からの参戦は違法とされているにもかかわらず参加者がいることが報じられている。[20]

能動的サイバー防御に政府が前のめりになるということは、こうしたサイバー戦争の多くの民間人を巻き込むことを意味するだけでなく、参加の動機をもさせるようなサイバー戦争のためのプロパガンダもまた強化されることになる。サイバー攻撃が繰り返され日本が被害者であるという不安と怒りを煽るような情報環境が情報戦として展開されることにもなる。

## 9．日米同盟のなかでのサイバー攻撃への加担と責任

「提言」で言及がないもう一つの重要な問題が日米同盟などいわゆる同盟国とか友好国などとされる諸国との関係におけるサイバー領域の連携である。日本がアクセス・無害化攻撃を展開する場合に、日米同盟などとの連携がどのように行なわれることになり、その場合の日本の責任(アトリビューション)どのように判断されることになるのか、など国際紛争における重要な問題への基本的な認識が示されていない。

日米安全保障協議委員会（「２＋２」）の協議において、サイバー領域が日米安全保障条約第５条の対象に含まれるということが確認されたという報道がなされている。2023年1月11日の2+2の会合の声明では以下のように述べられた。

> 閣僚は、同盟にとっての、サイバーセキュリティ及び情報保全の基盤的な重要性を強調した。閣僚は、２０２２年３月の自衛隊サイバー防衛隊の新編を歓迎し、更に高度化・常続化するサイバー脅威に対抗するため、協力を強化することで一致した。米国は、より広範な日米協力の基盤を提供することとなる、政府全体のサイバーセキュリティ政策を調整する新たな組織の設置及びリスク管理の枠組みの導入など、国家のサイバーセキュリティ態勢を強化する日本のイニシアティブを歓迎した。閣僚は、日本の防

18 https://www.cambridge.org/jp/universitypress/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB

19 2022年段階の記事によると、ウクライナの戦争では、ロシアが傭兵を積極的に投入していることが知らているが、ウクライナもまた52カ国から約4万人が義勇兵として申し出ており、ウクライナ領土防衛国際軍団に参加した。ウクライナのIT軍への参加呼びかけのツイートには、30万人が返信しているという。Ann Väljataga、"Cyber vigilantism in support of Ukraine: a legal analysis" March 2022 https://ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-a-legal-analysis.pdf

20 (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/

> 衛産業サイバーセキュリティ基準の策定に係る取組を含む、産業サイバーセキュリティ強化の進展を歓迎した。そして、閣僚は、情報保全に関する日米協議の下でのこれまでの重要な進展を強調した。

この文言をアクセス・無害化というサイバー先制攻撃を可能にしようとしている日本政府の方向性を見定めながら読む必要がある。また、2024 年 7 月 24 日の 2+2 の声明では以下のように述べられている。

> 日米は、相互運用性の深化を実現するため、強固なサイバーセキュリティ及び情報保全並びに情報共有の重要性を認識するとともに、情報共有の機会の増加、サイバーセキュリティ、データセキュリティ及び情報保全の更なる向上並びに通信及び物理面でのセキュリティの強化を検討する。（中略）閣僚は、同盟にとって、また、同盟が未来志向の能力を開発し増大するサイバー脅威に先んじるために、サイバーセキュリティ及び情報保全が基盤的に重要であることを強調した。閣僚は、情報通信技術分野における強じん性強化のためのゼロ・トラスト・アーキテクチャの導入を通じたサイバーセキュリティ、情報保全に関する協力の深化にコミットした。閣僚は、重要インフラのサイバーセキュリティの強化の重要性について同意し、同盟の抑止力を更に強化するため、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の促進について議論した。米国は、情報共有のためのより良いネットワーク防御の実現に資するリスク管理枠組みの着実な実施を含む、国家のサイバーセキュリティ態勢を強化する日本の取組を歓迎した。閣僚は、将来の演習にサイバー防御の概念を取り入れる機会を増やすことについて議論した。閣僚は、二国間のサイバーセキュリティ及び情報保全に関する協議を通じてなされた重要な進展を称賛した。

上にある「増大するサイバー脅威に先んじる」とか「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の促進」といった文言に含意されている内容に、サイバー攻撃の意図が含まれていないと解釈することは難しい。安全保障関連の文書の「防衛」とか「防御」という文言は、文字どおりの意味ではなく力の行使や威嚇を自衛権行使として国際法上正当化するための言い換えであって、実際には攻撃という含意だと解釈すべきだろう。

サイバー領域での抑止力にはサイバー攻撃を未然に阻止することもまた抑止力として効果をもつという解釈がありうることも注意したい。相手の攻撃を抑止するための先制攻撃がサイバー領域で実行されることは、前述した米国のイランへのサイバー攻撃ですでに行なわれた実績がある。サイバー領域における攻撃は、実空間での力の行使を阻止するという口実で正当化されやすいし、その実行に対する世論の批判もかわしやすい。この意味でもサイバー攻撃はハードルの低い手段である。このことを踏まえて米軍との連携がサイバー領域で展開されるということは、力の行使や威嚇のハードルの低い領域で日本が参加しつつ、結果として実空間での武力紛争に関与する結果になる、という可能性が高い。[21]

いずれにせよ、「提言」の枠組では、日本の米軍基地は重要な役割を担うとともに米軍との一体化が進む自衛隊が巻き込まれるだけでなく積極的にその役割を担い、米国のビッグテックがサイバー戦争の担い手である以上日本側の通信事業者もまた積極的な関与が可能なように企業体制の見直しも進められるはずだ。これまでの戦争で日本が後方のロジスティクスなどを担うことがあったが、サイバー戦争ではむしろ日本が攻撃の主体を担う可能性がより大きい。ただし、上に述べたことの殆どは事前に公表されることはないだろうし、そもそも日本に攻撃が帰属するという痕跡すら残されな

21 抑止力という言葉が核兵器であれば、核の使用の絶対的な阻止を意味し、通常兵器であればその使用が一定程度あったとしても、ある規模以上の使用を断念させるだけの武力の行使という意味の抑止力が含まれるから抑止力=武力の不使用を意味しない。

いだろう。

## 10．憲法9条と国際法――サイバー戦争の枠組そのものの脆さ

「アクセス・無害化」の先制攻撃という発想がでてくる背景には、自衛のための武力行使は国際法上も正当であり、かつ、憲法9条もまた自衛権としての戦力の保持を認めている、とい自衛戦争肯定論がある。自衛権の行使は相手の武力行使という事実があって、これへの正当な反撃としてなされるものだ、というのが従来の基本的な考え方だった。しかし現在ではむしろ、ロシアのウクライナ侵略のように、先制的な攻撃によって相手の武力行使を抑え込むことも自衛の手段とみなされるようになっていると思う。しかしこうした先制攻撃は相手の自衛権行使を正当化することでもあり、その後の武力行使の応酬と戦争の泥沼化に繋がる。

サイバー領域は、とくに、実空間での物理的な破壊のようなリアリティが乏しく「戦争」というイメージをもたれにくいために、サイバー攻撃の敷居は低い。しかも秘密裡の攻撃が常態となっていることから、戦争に関する法手続きや民主主義的な討議の余地も小さくなる。それだけではなく、情報戦を通じた世論の敵意醸成や偽情報の拡散などといったサイバー領域の敵対的な感情の扇動が行なわれる結果として、外交的な手段であるとか、政府とは別に、市民レベルでの相手国との交流や反戦運動などの可能性が著しい困難に直面する。こうした副作用も含めてサイバー領域での自衛戦争の弊害をきちんと理解する必要がある。この点を理解すれば、私たちがとるべき選択肢は一つしかないことがわかる。それは、「提言」が提起する情報通信領域の網羅的な監視に明確に反対し、グローバルな「通信の秘密」を断固として主張することであり、自衛の手段としての先制攻撃も、サイバー領域におけるスパイ活動やハッキングを含む一切の「アクセス・無害化」の権限も、政府に与えるべきではない、ということである。

「提言」が憲法9条に言及せず、戦争を禁止する国際法への配慮もないこと無視できない重要な問題だ。憲法9条も国際法上の戦争法や関連する法規の基本的な枠組ができあがって時代には、インターネットもサイバー領域における力の行使や威嚇といった問題が存在していなかった。とはいえ、とりあえずインターネットなどグローバルなサイバー空間にも国家主権が及ぶとみなして、従来の国際法の枠組を無理矢理当て嵌めようという努力が行なわれてきた。しかし、従来の解釈をそのままサイバー領域に当て嵌めることが困難な場合が多くみられる。このために、サイバー領域における力の行使の何が国際法や戦争法に照らすて合法なのかの国際的な合意が存在するのかどうか極めて曖昧な状況にある。こうしたなかで、各国政府が自分に都合のよいように解釈し、その解釈を国際標準として認めさせようとする法の正当性を巡るヘゲモニー争いが起きているともいえる。

各国とも、自国の軍事力や安全保障政策にとって有利なルールを主張している状況は、事実上サイバー攻撃は何でもアリ、という危険な兆候を孕んでいるともいえる。だから日本政府は、この混乱に乗じてサイバー領域における戦争を自らに都合のよい枠組で正当化するための法整備に前のめりになっているのだろう。革新野党が、ここでもサイバー攻撃の不安感情にとらわれた世論や有権者の支持を失ないたくない一心で、サイバー攻撃に対する何らかの力の行使や威嚇の必要性を認めかねない、と私は危惧している。これに対して私たちは、明白な力の行使や威嚇を一切認めない立場をとることで、はっきりと対立点を提起してサイバー領域を明確に戦争から切り離す方向を提起すべきだ。この場合、その核心をなすのが、自衛権という名の力の行使や威嚇も明確に否定することにある。むしろ実空間とは違って、サイバー領域のセキュリティは力の行使や威嚇ではない別の手段で、国家に委ねることもなく、コミュニケーションの主体である私たち自身が自らの手で防衛できる領域でもある。コミュニケーションを国家や営利企業の支配から切り離すことは、同時に、サイバー領域の平和構築の基盤を構築することになるはずだ。

# 2025年1月JCA-NETセミナーのお知らせ

## 1月25日(土)15時から　サイバー安保批判の基本

開催方法：オンライン
(申し込み方法は最後をごらんください)

現代の戦争は、情報通信、AI、ビッグデータと一体化した従来では想像すらできなかった事態になっています。戦時と平時の区別は消し去られ、戦闘員と非戦闘員の区別もなく、誰もが標的にされ、誰もが戦争の加担者になりえます。場所と時間の区別もないまま、従来の国際法のルールを無視した様々な手法での先制攻撃を仕掛けるのが当たり前になりつつあります。

政府は、経済安保によって経済活動を軍事・国益に統合する枠組を構築し、マイナンバー/カード体制によって人々の日常生活の監視を制度化して国策への動員の基盤を構築してきました。サイバー安全保障は、一方で武器のIT化を推進し、他方でサイバー攻撃への不安の扇動と虚実ないまぜのプロパガンダにSNSを動員する体制の構築が目指されています。こうして、私たちの言論・表現空間が戦争に巻き込まれはじめています。

今回のセミナーでは、11月末に出された政府有識者会議の提言「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」を批判的に検討します。この提言を踏まえて25年の通常国会では、具体的な法整備へと向かうことになります。「サイバー」の分かりづらい議論に翻弄されずに、サイバー戦争反対の核心を突いた批判の観点を皆さんと議論します。

参考

サイバー安全保障「提言」批判
https://www.alt-movements.org/no_more_capitalism/blog/2025/01/22/cyber-anpo_teigen_hihan/
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(有識者会議)
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen…
(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の平和を
https://www.jca.apc.org/jca-net/ja/node/296

## セミナー：1月28日(火)19時から　フォローアップ

開催方法：オンライン
(申し込み方法は最後をごらんください)

毎月最後の回は、特にテーマを設けずに、参加者の皆さんが持ち寄った様々な疑問や質問、あるいは意見などをとりあげながら進めています。毎回のセミナーでは十分に取り上げられなかった課題や消化不良になった話題について、補足の説明などにあてる場合もあります。

最近の社会・政治的なテーマでセミナーやメーリングリストなどで話題になった事柄の一例。
- ガザ戦争とIT産業の戦争責任
- 能動的サイバー防御とサイバー安全保障
- 生成AI
- 国連サイバー犯罪条約
- マイナンバーとデジタルID

- 政府による暗号規制
- ジェンダーとインターネット
など。

4 参加方法
==========

JCA-NET の会員以外の方でセミナーに初めて参加される方は予約が必要です。

下記の申し込みフォームから申し込んでください。(アクセスに若干時間がかかるかもしれません) 右の QR コードからもアクセスできます。
https://pilot.jca.apc.org/nextcloud/index.php/apps/forms/s/EJWYbsArEEc4tD9Hnj3rcz4E

あるいはメールで申し込む場合は
jcanet-seminar@jca.apc.org
まで以下の各項目を記載して申し込んでください。

申し込み内容
- おなまえ
- メールアドレス
- 参加希望のセミナー番号(複数可)
- 今後もセミナーの案内を希望するばあいは「案内希望」とお書きください。
- セミナーのメーリングリストに参加希望のばあいは「メーリングリスト希望」とお書きください。

参加費 無料(カンパ大歓迎)

オンラインは Jitsi-meet を使用します
オンライン会議室 Jitsi-meet のマニュアル
https://www.jca.apc.org/jca-net/ja/node/93

JCA-NET の会員メーリングリスト、セミナーメーリングリストに登録されている方は、当日 30 分前に、メーリングリストからの会議室案内をみてアクセスしてください。

---
余裕のある方は是非カンパをお願いします。
セミナーは JCA-NET の会員の会費で運営されています。
郵便振替口座
ＪＣＡ－ＮＥＴ （ジ゛ェイシーエイーネット ）
記号番号：00190-3-417584
ゆうちょ銀行〇一九店 417584

# 映画『10 月 7 日からの Gaza』の試写会とトークイベント

映画『10 月 7 日からの Gaza』の日本語字幕版の試写会とトークイベントを開催します。

●開催日時

## 10.1.1. 2 月 9 日(日)映画上映 15 時から

トークは映画終了後(トークのみの参加も可能です)
開催方法 オンライン、予約が必要です(以前の試写会に申込まれた方も再度予約が必要です。) 参加費：無料(カンパ歓迎)

予約は下記のフォームから申し込んでください。
https://pilot.jca.apc.org/nextcloud/index.php/apps/forms/s/CJBWSsr57LNJBSX2yJCJYJsp

上映後のトークイベント

上映終了後の 16 時 45 分頃から下記のトークイベントを開催します。パレスチナとイスラエルをめぐる背景などについて、ゲストからお話をいただきます。

お話：田浪亜央江さん

プロフィール
中東地域研究。ヨルダン川西岸地区とイスラエル領内のパレスチナ人の文化を通じた抵抗運動に詳しい。広島市立大学教員として 2017 年より広島在住。2023 年 10 月以降、ガザのジェノサイドに抗議して原爆ドーム前でスタンディングを行う「広島パレスチナともしび連帯共同体」に参加。お話の後で若干の質疑の時間をとります。
問い合わせ先 小倉利丸(JCA-NET) toshi@jca.apc.org 070-5553-5495

●映画の概要
この映画は、ジャーナリストであり国会議員でもあるアイメリック・カロンがガザ現地のジャーナリストと連絡を取りながら、映像の確認、選別、日付の記入を行って制作された作品。更に、この映画では、これらのガザのジェノサイドの生々しい映像に割り込むようにして、イスラエルの政治家たちの演説、イスラエル兵が SNS に投稿したガザのビデオ映像などが挿入される。

この作品は、フランス 国民議会で国会議員らを招待して 5 月 29 日初上映されたが、出席した国会議員はわずか 17 人。その後、カロンは、Les Mutins de Pangee で無料で公開している。

内容は、日本のメディアでは絶対に報じることができない文字どおり目を覆いたくなるシーンの連続だ。しかしこれらの映像は、ジェノサイドの事実の一部であり、ここから私たちは目を逸らしてはならないだろう。 公式サイトは「これらの映像は、民主主義国家において、自称 "世界で最も道徳的な軍隊 "が犯した戦争犯罪を記録している。」「アメリカと EU、特にドイツ、さらにはフランスから大量に供給された武器で行われた犯罪である」とし、次のように書いている。

「見始めて最初の数分間で、この映画が止まってほしい、すぐに終わってほしい...犯罪が止まってほしい、銃撃が止まってほしい、すべてがなかったことになってほしいと願うだろう。 この映像を見て、誰がこれらの犯罪を否定したり正当化したりできるだろうか？ 私たちは、毎日消化を強いられる大量の映像にひたるなかで、映像がもはやさほどの重みも持たず、現実が平然と否定され、あるいは公然と軽蔑されることを当たり前とするような悪意に対して、これに反対する言葉を見つけることができていない。戦争犯罪人とその共犯者たちは、自分たちが引き起こした死者だけでなく、歴史を通じて反ユダヤ主義の犠牲となった人々の記憶をも汚そうとしている。これらの映像は、何よりもまず、こうした事態に歯止めをかける必要性があることを証している。このような犯罪を支持し続ける人々、憎悪、復讐、非人間化の演説に直面するとき、言葉による一騎打ちに引きずり込まれるよりも、私たちはこの一方通行の映像という鏡を掲げたい」

映画試写会の主催 JCA-NET https://www.jca.apc.org/jca-net/ja