「兵役拒否・平和主義・エキュメニズム」研究会

ハイブリッド戦争時代のサイバー戦争と「武力行使」概念の課題

中西　久枝

はじめに

アメリカとロシアがウクライナを巡り対立を始めてから十数年が経過した。ロシアのウクライナへの軍事侵攻が刻々と激化している。欧州諸国がこうした状況にどう対応するのか、喫緊の問題となっている。2010年以降、欧州では徴兵制の復活の動きが徐々に進みつつあり、エキュメニズム（キリスト教の党派を超えた結束を目指す運動）の思想や兵役拒否の思想とその実践はこれまで以上に重要性を増している。兵役の担い手が戦闘員及び市民（国際法上は文民）に対する虐殺や人権侵害の一端に関わる外的条件が揃っているからである。

他方、兵役が担う戦闘及び非戦闘行為とは何か、という本質的な問題は今日急激に変化している。情報技術とAI（人工知能）の飛躍的発展により、サイバー空間が非軍事的、軍事的に活用される時代になっているからである。武力紛争下で適用される国際法である武力紛争法をサイバー攻撃やサイバー戦争にどう適用するのか、従来の解釈では決定できない事態が、今日生じている。武力紛争法は、武力紛争の際適用される原則や規則を定めており、戦時下においても人道を基本原則として掲げ、戦闘行為の実施者の行為を規制している。しかしながら、サイバー攻撃の実施者が戦闘員なのか、文民とみなされるべきか、国際法的な基準がいまだに整備されていない。

こうした状況下、兵役に服する者がサイバー戦争の一翼を担う場合、サイバー攻撃の存在を国家がどのように判定し報復をするのか、またその報復行動が国際法上許容される範囲なのかなど、さまざまな課題が浮き彫りになっている。

本稿では、まず「武力行使」禁止に関わる国際的な規範化がどのように展開してきたかをふりかえり、サイバー攻撃やサイバー戦争がおこる以前の武力行使の禁止あるいは容認について、第二次世界大戦から今日までの武力行使の概念とその実施の様相を再考する。そのうえで、2節ではサイバー攻撃、サイバー戦争の定義とその多発化の背景について論じる。3節では、サイバー空間を利用したサ

イバー戦争がどこまで武力行使だとみなされるべきかの国際的な議論と動向について、4節では「サイバー行動」（Cyber Operations）という、サイバー攻撃やサイバー戦争より包括的な概念がどのように登場し、国際的に規範化する動きとなっているかを分析する。そのうえで、ハイブリッド戦争時代のサイバー戦争が兵役者のみならず一般市民に対して突きつけている課題、特に武力行使の荷担に巻き込まれるリスクについて問題提起を試みる。

1. 問題の所在―第二次世界大戦後の「武力行使」禁止の規範化と「武力」の行使

20世紀の前半は、2つの大戦という悲劇的な戦争を人類は経験した。戦間期には戦争の違法化に関する国際的な取り組みが試みられたが、第二次世界大戦は、ヨーロッパのみならず日本を含むアジア諸国に至るまで甚大な被害をもたらした。そうした反省から、第二次大戦後設立された国際連合は、「武力行使」の禁止を憲章第2条4項明確に規定した。憲章には「戦争」という用語は使われていない。また憲章は、明確な軍事力の行使を指す事がらに関しても「武力行使」という術語で規定しているが、原則的に武力行使を禁止する精神に裏打ちされている。

武力行使とは何を指すのか、実はいまだに国際法学者、国際政治学者、実務家のあいだで意見が分かれている[1]。他方、国連憲章で謳われている武力行使の概念は、平時と戦時を問わず人間の尊厳を保護する目的のために、国際条約や国際紛争処理の過程で発生した判例などを総合し、国際法として発展してきた。その中で特に武力行使に関わる国際法として、国際人権法と武力紛争法（交戦法規 と中立法規 から成る国際連合憲章 以前の戦時国際法）がある。国際人権法は、国際法の中の人権に関わる法であり、1948年の世界人権宣言をはじめ、難民や無国籍者の保護、人種差別の禁止、女性・子ども・障がい者の権利の保護などを規定するさまざまな条約から構成されている。

他方、武力紛争法は、戦時における法であり、武力行使の発動のあり方を規定した国際条約を結集したものである。ともに個人の保護を目的としている点は共通しているが、武力紛争中においては戦闘員の生命をも守ることが重要であるという人道主義の立場に立脚している。一方、武力紛争法は、武力紛争下での死傷者や破壊を最小限に喰いとめるために発展してきた点は看過できない[2]。

国連は紛争がおこったときは、まず平和的解決を追求することを憲章6章で期している。平和的解決が遂行できない事態になった場合は、憲章7章で「強制行動」を取りうることを規定し、経済制裁もしくは国連軍の派兵が安全保障理事会の決

議をもって可能であるとしている。冷戦後の国内紛争、内戦などが頻繁におこるようになってからは、平和維持活動（Peace Keeping Operation）がさかんに発動された。この平和維持活動は、憲章6章にも7章にも規定のないものであり、いわばその都度方式の平和維持軍の派兵である。武力行使禁止の例外的な領域としては、国連憲章上は自衛権の行使と集団的自衛権の2つのみである。こうした例外を除けば、国連が軍事力を行使できるのは、憲章7章の規定する国連軍の派遣のみである。しかし現実には、安全保障理事会の決議が採択されれば、有志連合軍の性格の強い平和維持軍が派遣され、その数は1988年から1994年のあいだのみで20に増えた。平和維持活動は、その後平和構築活動という枠組みで活動内容が拡大したが、成功例は東ティモールくらいであると言われている[3]。

2001年の9.11事件以降、正戦論がアメリカの外交及び安全保障政策の中で新たに再解釈され、「テロとの戦い」の名のもと、武力行使が正当化される傾向が強まった。それは、2001年の対タリバン戦争と2003年のイラク戦争に如実に現れた。対タリバン戦争の場合は、国連安全保障理事会（以下、安保理）の決議を経ている一方、イラク戦争の場合は、安保理決議の正式な許可を得ない「侵略」戦争であった[4]。他方、いずれの戦争も、約20年近く経過した現在も、戦後復興からは遠い状況となっている。このことは、安保理決議という国際的な「お墨付き」のある武力行使であっても、国際法上違法行為である侵略の場合（2003年のイラク戦争）でも、行使された武力がもたらした代償は、当該諸国にとっても国際社会にとっても大きいことを示している。

冷戦後のもう一つの武力行使の実態として、「人道的介入」がある。この概念のもとで国際的な軍の派兵は、1999年のコソボ戦争などがあるが、その後は2005年10月に国連首脳会合成果文書として「保護する責任」の文書が採択され、2006年の安保理決議1674号の採択の経緯などを踏まえ、非戦闘員（文民）の保護という「人道的」目的のために集団的安全保障の枠組みの中で、「被介入国の同意なしに武力を使用して実施する強制的活動」が実施されることが許容された。近年の事例としては、2011年のアラブの春後の混乱期に実施されたリビアへの「人道的介入」が最後となっている。コソボ戦争の場合もリビアへの人道的介入に対して介入の正当性については評価が分かれている。評価の基準は多様であるが、その中で重要な指標としては、介入の前夜のリビア内の人権違反行為の所在や介入時の反政府軍の活動と政府軍の市民への攻撃の度合い、さらには介入の結果起こった体制転換がその後の国民和解に与える影響などが重要であると指摘されている[5]。

また、リビアへのNARTO軍の介入は、NATO軍の状況認識の誤りが招いた拙速な軍事行動であったという見方が現在主流化しつつある。コソボ紛争への介入は、人道的介入の概念が国際的に「保護する責任」の一部として規範化した2005年以前に起こった事例であり、リビアの事例はその後の国際法化後という違いはある。しかし、いずれの場合も国連の安保理決議を経た軍事行動とはいうものの実際にはNATO軍が派兵している点で共通している。

国連憲章では、憲章2条4項において、武力行使のみならず「武力による威嚇」をも禁止している。その例外は、先述のように基本的には自衛権の行使と集団的自衛権の場合の2つである。しかしながら、冷戦後から9.11事件を経て、さらにアラブの春後のリビアへのNATO介入というプロセスから見えるのは、軍事力が国連憲章7章の規定する強制行動の枠を超えて行使されている現状である。人道的介入は、文民の保護という目的に根差している一方、国家主権への「不干渉」原則を侵害する干渉・介入行為である。こうした干渉は今後も続くのだろうか。今後リビアの事例に類似したケースが安保理で採択される可能性はそれほど高くないという見方が多く、人道的介入の憲章上の位置づけについては、憲章7章に基づいた軍事行動であると捉えるのは無理があるといわれている[6]。その意味でも、ポスト冷戦期以降の今日までの30年間、国連憲章にはもともと規定がない概念（平和維持軍、人道的介入、保護する責任）が常任理事国の意向が強く反映して規範化され、軍事力という武力行使が国際的に進んだ点は否定できない[7]。

では、リビアへの介入後から今日までの動きはどうであろうか。人工頭脳に関わる急速な技術革新によって、サイバー戦争と呼ばれる新たな戦争が国際社会に影を落としている。それでは、この新たな戦争形態は、国連を中心に展開してきた（あるいは無視されて来た）「武力行使禁止原則」に照らし合わせたときに、どのように位置づけられるのだろうか。次節では、まずサイバー戦争とは何か、サイバー戦争が新たな戦闘様式として重要性を持つに至った背景は何かを明らかにする。

2. サイバー攻撃、サイバー戦争の多発化とその背景

サイバー戦争という用語については、まずサイバー攻撃とサイバー戦争の違いを明確にする必要がある。サイバー攻撃については、「政治的あるいは国家安全保障にかかわる目的で、コンピュータの機能を破壊する行動」を指すというハサウェイの定義が一般的だとされている[8]。しかしながら、ネット上で行われるすべての破壊的行為や情報工作が、サイバー攻撃だというわけではない。クレジットカード

情報の窃取や改ざんなど、単に金融上の利益を目的とした行為は、サイバー攻撃の定義に当てはまらないという見解が主流となっている[9]。サイバー攻撃と呼ぶには、攻撃の手段、目的（目標）、効果などの面で、政治目的あるいは攻撃相手の安全保障上の危害を目的とする意図が存在していることが条件となる[10]。また、サイバー攻撃が行使されても、それがただちにサイバー戦争になるわけではない。確かに、ICTによって制御された無人飛行機が爆弾を投下したり、ミサイルを搭載して攻撃したりするような場合は、物理的な被害（kinetic damage）を与えるため、通常戦に近い戦闘行為とみなされ、サイバー攻撃にはならない[11]。

他方、サイバー攻撃が重要インフラを標的にし、たとえばイランの核施設の制御装置が破壊されウラン濃縮に必要な遠心分離機に障害が起こった事例や[12]、アメリカ政府職員の約400万人の機密情報が窃取され、システムの回復に数十億ドルを要した事例のように、極度に被害が大きく、また攻撃の意図が政治的な場合には、サイバー戦争と呼ぶのが適切だと言う指摘がある[13]。そうした議論の突破口を開いたのは、塩原によれば、クラークらによる「サイバー戦争」という本であったという。サイバー戦争は、「損害ないし破壊を引き起こす目的のために他の国家のコンピュータないしネットワークに侵入する国民国家による行動」だとクラークは定義している[14]。この国民国家という表現は、コンピュータやネットワークに侵入をした行為者の背後に、国家の指揮･命令が存在することを含蓄している。つまり、ある個人がそうした侵入行為を実施したとしても、それがある国家の政治的あるいは戦略的な意図が背後になければ、サイバー戦争とは位置づけないのである。

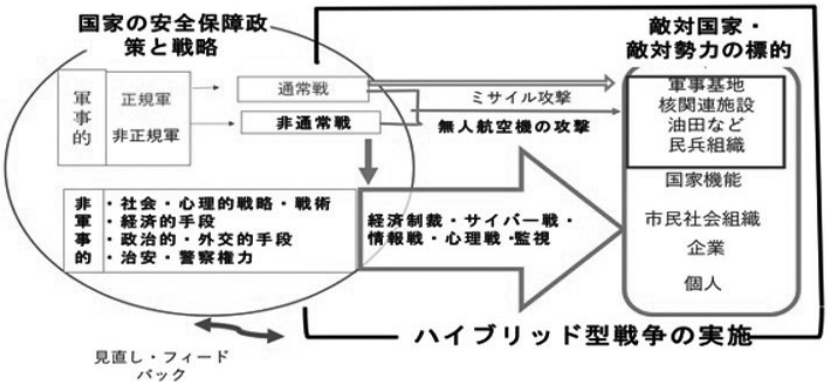
また、サイバー戦争が起こる前提として、ハイブリッド戦争があることはこの10年間の研究で明らかになっている。ハイブリッド戦争は、その先駆的な研究では、いわゆるならず者国家がゲリラ戦と同様に採用する通常戦と非通常戦の組み合わせだと定義されている[15]。その後、ハイブリッド戦争は、2014年以降のロシアによるクリミア半島及びウクライナ東部への介入に採用された戦争だと捉えられてきたが[16]、定義はいまだに分かれている。最近ではハイブリッド戦争とは「正規戦、非正規戦、人工知能（AI）の活用によるサイバー戦や情報戦など複数の手段を駆使した戦争」であり、「全面戦争を意図せず、AI技術によるサイバー攻撃やインターネットの情報を駆使することで、相手に安全保障上のダメージを与え、自国の政治目標を達成しようとする新しい戦争」だと言われている[17]。

従来、戦争が武力を伴う戦闘を指すのに対し、ハイブリッド戦争は、ミサイルや爆弾などの動きのある（kinetic）武力行使を伴わない闘いをも含む点で、従来

の戦争の概念を超えている。従来、武力行使とは、他国の 領土 や 軍隊 を砲撃したり、他国の 港湾 を封鎖したりするなど，国際関係において 武力 に訴えることを指し、敵の兵力に対し殺傷・破壊を目的とする戦闘行為を行うことであるとされている。これは通常戦を前提としている。

サイバー戦争の「武力性」についてはいまだに論争中である [18]。ある行為が武力行使であることが明白なのは、軍事攻撃や軍の派兵であるが、サイバー戦争はとかく通常戦を補完する形で、ハイブリッド戦争の一端をなす戦闘として実施される [19]。それを図で示すと以下のようになる。

ハイブリッド型戦争の実施・展開図



[出典：筆者作成]

上図のようにサイバー戦が通常戦と組み合わせて実施された事例として有名なのは、先述のようにロシアによる 2014 年のクリミア併合とウクライナ危機である [20]。

ハイブリッド戦争の場合、たとえば無人航空機をサイバー上で操縦したり、それにミサイルを搭載したりしつつ、敵対勢力や敵対勢力の施設に攻撃を行うことがある。無人航空機の操縦者が民間人である場合、単なる偵察をした場合と無人航空機を使用して「空爆」した場合とでは、サイバー行動の戦闘性も目的も効果も異なる。つまり、戦争を起こす主体は軍事的行動をとったのか、ミサイルが搭載されていなければ非軍事的な行動とみなすのかなど、軍事、非軍事、軍人、民間人の明確な区別をどう決めていくのかは難しい問題である。

さらに、標的が軍用物なのか、民用物なのかという区別は、これまでの武力戦争法の捉え方では十分にできない〈後述〉。ハイブリッド戦争を構成するサイバー

戦争が標的にするのは、国家、国家機能、市民社会組織、企業、個人など、いわゆる軍事施設や戦闘員とは異なる場合が存在するからである。

3. サイバー攻撃、サイバー戦争は、どこまでが「武力行使」になるのか
―サイバー空間をめぐる議論―

サイバー戦争において、どこまでが武力行使に当たるのかを捉えるには、まずサイバー空間とは何かを考察する必要がある。サイバー空間については、アメリカ政府、イギリス政府、カナダ政府などが様々な定義を提出しており、必ずしもコンセンサスは得られていない。ここでは、その中でやや幅広い定義をしているカナダ政府のものを引用してみる。カナダ政府は、「情報技術の相互に結ばれたネットワークおよびそのネットワーク上の情報によって創造される電子世界」と捉えている[21]。しかしながら、この定義では、サイバー空間にはどの国家が所有し、管理するかという国家主権の問題が想定されていない。実際には、電子世界を構成するインフラまで含むかどうかによって、国家主権がどこまで及ぶかが決まる。かつては、サイバー空間には、領土に基づいた境界はないと主張する立場もあった。しかし今日では、ジョセフ・ナイが主張するように、サイバー空間に物理的インフラ層とヴァーチャル層ないし情報層があるという主張の方が有力になっている[22]。

塩原俊彦氏によれば、サイバー空間にインフラを含める立場は、サイバー空間を「戦場」と捉えるものだとし、逆にインフラを排除する立場をとるとサイバー空間を「平和の場」と考えることになると言う[23]。サイバー空間を戦場と考えると、国家が外敵からの脅威に晒されないようにサイバー関連のインフラをどのように防衛するのか、という命題が出てくる。それは、サイバー空間が国家安全保障上の脅威になりうる場であるという認識につながる。

他方、サイバー空間を「平和」と捉える考え方は、インターネットの活用が利用者の善意に基づくことを前提に普及ししてきた経緯に依拠するものであり、人びとの良心によって「平和の場」になりうる可能性を模索した動きにみえる。しかしながら、実際には、前者の立場の方が今日優勢となっている。それは、2005年におきたスタックスネットというワームによる攻撃をはじめとして、今日多くのサイバー空間上への攻撃が増えていることと関係している。またアメリカをはじめ北太平洋条約機構（NATO）は、サイバー攻撃がもたらす被害とその効果が大きいとみなす立場を採っていることも影響している。その背景には、アメリカとロシアの緊張関係がある。アメリカがサイバー攻撃に対する防衛体制や攻撃す

る能力など、サイバーセキュリティ能力の強化を認識したのは、対ロシア戦略ゆえである。サイバー攻撃能力の高度化に早々と成功したのはロシアであり、そのロシアはトランプ大統領が勝利した大統領選挙の過程で投票活動に影響を及ぼすサイバー攻撃を実施したといわれている。

それでは、サイバー攻撃を受けた場合、それが国家主権の及ばない外部アクターによるものであった場合、どのような国際法が適用されるのだろうか。端的には、国際条約、慣習法のいずれにおいても、適用可能な国際法はまだ十分に確立されていない。民間企業がネット上の攻撃を受けた場合と異なり、国家の安全保障にかかわるインフラに相当規模の破壊が及んだ場合、そうした攻撃が武力行使に値するのかという点について、国際的な合意はない。

武力紛争下においては、戦闘員と文民は区別され、また軍用物と民用物の区別を明確にすることで、被害者をいかに保護するかという努力がこれまでも行われて来た。1977年のジュネーブ条約の追加議定書Ⅰは、文民と民用物は攻撃対象としてはならないことを明確にしたことは重要である。

他方、サイバー攻撃が頻発している状況下、国連総会での政府間プロセスの場において、法制化に向けた会議が開催されている。政府専門家会合やオープンエンド作業部会などがその主な動きである。参加国数は、2004年に始まった第1回目から徐々に増加し、第6回の2019年～2021年の政府専門家会合では、サイバーセキュリティをめぐって議論されてきた。

国際法がどのようにサイバー空間に適用されうるかは、2014年～2016年の第四回会議になって初めて議論され始めた。特に国際法の中でも武力紛争法という戦時に適用される法がいかに適用されるかが焦点となってきた[24]。武力紛争法はサイバー戦にも適用されるべきだとする国の方が、全体として圧倒的に多い。逆に、適用されるべきでないと主張する国家は、中国、キューバ、イラン、ニカラグア、ロシア、ベネズエラなど、アメリカの覇権主義に反対する国家群に集中している。

中国はサイバー攻撃をいかに予防するかに重点を置くべきだという立場をとった。サイバー攻撃の予防は、サイバー攻撃の防衛とは異なる。予防は、国際社会がいかにサイバー攻撃を互いに回避するかという問題である。いいかえれば、サイバー攻撃が一つの武力だとすれば、攻撃はどのような場合に発動してよいかという、通常戦下の武力行使の発動に関わる問題を議論する動きが、中国を中心に始まっているのである。

国際的な議論が国連を中心として展開するなか、赤十字国際委員会が提出した報告書が注目される。それは、武力紛争法の持つ具体的な観点、たとえば許容さ

れるべき攻撃対象など攻撃側の予防原則や防衛側の予防原則や文民たる住民に対する一般的保護などの観点から、サイバー行動[25]についての赤十字の見解を明確に述べているからである。

表　武力紛争法のサイバー行動への適用に関する赤十字国際委員会の立場

区　　分	赤十字国際委員会の見解
武力紛争法の一般原則 （データの位置付け）	今日の世界はデータに依存していることから、極めて重要な民用データの消去又は改ざんが武力紛争法上禁止されないと結論付けることは、武力紛争法の趣旨及び目的と一致しないであろう。
特別の保護対象 （医療組織の保護）	武力紛争中に医療部門に対してサイバー攻撃を行うことは、武力紛争法に違反する。
特別の保護対象 （文民たる住民の生存に不可欠な物の保護）	文民たる住民の生存に不可欠な物を攻撃し、破壊し、移動させ又は利用することができないようにすることは、武力紛争法によって禁止されている。
区別原則	・サイバー手段は、必ずしも無差別兵器ではない。カスタムメイドのサイバー手段であれば無差別になる可能性は低いと考えられる。 ・武力紛争法は、民生インフラ及びデュアルユースのインフラのうち軍隊が使用又は使用を予定していない部分に対する直接的なサイバー攻撃及び無差別サイバー攻撃を禁止している。
比例性原則	過度のサイバー攻撃は武力紛争法によって禁止される。
攻撃側の予防原則	武力紛争法上、紛争当事者には、サイバー攻撃を行う際、文民及び民用物への付随的損害を避け又は少なくとも最小化するよう、全ての実行可能な予防措置をとる義務がある。
防御側の予防原則	武力紛争当事者は、サイバー攻撃の影響から支配下にある文民及び民用物を保護するため、全ての実行可能な予防措置をとらねばならない。
文民たる住民に対する一般的保護 （軍事行動から生ずる危険からの一般的保護）	武力紛争法は、サイバー技術を用いて、文民たる住民の間に恐怖を広めることを主たる目的とする暴力行為又は暴力による威嚇並びに武力紛争法違反行為の助長を禁止している。

[出典 : ICRC Position Paper 2019[26] 及び鳥居「サイバー攻撃の武力紛争法上の課題」（2021 年）112 － 113 頁をもとに筆者が編集]

では上の表では、赤十字国際委員会は、どの程度サイバー攻撃を武力行使と同じく禁止しようとしているのだろうか。攻撃を行使する側に対して禁止すべきだ

としているのは、無差別サイバー攻撃と過度のサイバー攻撃である。さらに、攻撃側には、文民及び民用物への付随的損害を避け最小化することを義務付けている。また、文民への一般的保護としては、恐怖を広めることを目的とする暴力行為あるいは暴力による威嚇も禁止としている。では、暴力行為または暴力による威嚇は、サイバー技術を駆使したときにどのような事態や状況を想定していると捉えるべきなのだろうか。こうした問題も、今後の基準づくりが求められるところである。

4.「サイバー行動」の国際的規制と課題

前節で述べたように、赤十字国際委員会の立場には、サイバー攻撃の実施主体に対する禁止条項の規範化であり、武力紛争法の文民保護の規定をサイバー攻撃に積極的に運用するニュアンスが感じられる。それに対し、こうした見解とは逆行する潮流が見られる。最近の動向として注目すべきなのは、サイバー行動を武力行使と同一化していく議論とそのマニュアル化である。サイバー攻撃が物理的な破壊（コンピュータシステムが破壊されても、コンピュータそのものは破壊されない）を伴わない場合「武力による威嚇または武力の行使の禁止」に相当する、あるいは近似するサイバー行動をどう回避するのか[27]、武力性を内包したサイバー行動を国際的にどう規制していくのか、今日国際的な場で議論されている。

その重要な動向の一つに、タリン・マニュアル及びその続編であるタリン・マニュアル2がある[28]。こうしたマニュアルが登場する以前から、国連の「国際安全保障の文脈における情報及び電気通信分野の進歩に関する政府専門家会合」（以下､国連サイバー GGE）という会合が2004年以来開催されてきた。しかしながら、ロシア、中国の意見が欧米諸国と分かれてきた経緯などにより、国連としてひとつの合意文書を作成するには至らなかった。それゆえ、エストニアのタリンにあるNATO サイバー防衛協力センター（CCD COE）が一部の国際法学者を動員してマニュアルを作成する事業を実施し、その結果生まれたのが、タリン・マニュアル（1と2）である。

エストニアはロシアからのサイバー攻撃を2005年に受けたことを鑑みれば、このマニュアルがアメリカの対ロシア政策の一環としてNATOが作成したこと、またそこには極度の政治性があることは自明である。問題なのは、日本の自衛隊も日米同盟という立場から、このマニュアルがまるで「国際法」的な位置づけにあるかのように、一般書として邦訳が出ている。

それでは、タリン・マニュアル2とはどのような内容なのであろうか。その特徴として、第一に、サイバー行動の「武力性」を強調している点がある。従来サイバー戦争の「武力性」についての議論の背景には、サイバー攻撃がもたらす有害性と効果（インパクト）―重大性―の観点から武力行使か否かを認定すべきだという主張がある。タリン・マニュアル2は、ある程度の「規模及び効果」を一種の重大性の基準としている。しかしながら、この重大性の基準は、どこまでがそれにあたるのかという点では今後の議論に任されている。その意味では。サイバー攻撃がサイバー戦争であると、つまり一種の「戦争」であると認定してよいかどうかは、その時々の状況と文脈と国家間のパワーによって変化する。これ自体が実は戦争なのか戦争でないのかの峻別がつきにくいことを意味している。

もう一つの特徴は、敵対国（タリンマニュアルはロシアが仮想敵国）のサイバー行動の破壊性に着目することで、サイバー行動を厳密な基準を設けずに武力行使と認定しやすくしつつ、集団安全保障の枠組みの中に位置づけようと試みている点にある。いいかえれば、武力紛争法の中の交戦法規にある「均衡原則」（戦闘が許される区域や交戦資格者についての原則）が吟味されることなく、サイバー行動を国連憲章の規定の違反行為と認定するリスクを秘めている。それは、戦闘員と非戦闘員の区別の問題にも影響する。

国際人道法では、文民と戦闘員の区別原則があり、「紛争当事者は、文民たる住民及び民用物を尊重し及び保護することを確保するため、文民たる住民と戦闘員とを、また、民用物と軍事目標とを常に区別し、及び軍事目標のみを軍事行動の対象とする」とジュネーブ追加議定書48条に規定されている。さらに、第51条4項では「無差別な攻撃は、禁止する。無差別な攻撃とは、、、軍事目標と文民又は民用物とを区別しないでこれらに打撃を与える性質を有するものをいう」と規定し、無差別攻撃を原則的に禁止している。

それに対し、タリン・マニュアル2では、「民用物とは軍事目標でないすべてを指す」と定義し、「軍事目標は、コンピュータ、コンピュータ・ネットワークおよびサイバー・インフラを含みうる」という[29]。軍用物の基準としては、軍事的利益の存在の有無や「軍事的活動に効果的に資する」かどうかを挙げており、ハードウェア、ソフトウェア、ウェブサイト、さらには電子メールも軍用物になりうると明示している。こうした考え方が、マニュアルを参照する国家にとって、サイバー攻撃の実施の際に活用されるのか、あるいは敵対勢力からサイバー攻撃があったことを認証するためのものなのかは、明確ではない。攻撃を受けたことを

決定する際の基準に使われるのであれば、「一個人のメールの内容も軍事的活動の一端をなす」場合があるという規則は、恣意的に運用される可能性は高い。メールの捏造は技術的に可能であり、「国家の安全保障に関わるため、メールの内容は公開しない」と宣言してしまえば、「サイバー攻撃」はあったと主張しうるのである。

タリン・マニュアル2では、文民が敵対的行動を採らない限り、攻撃からの保護を受ける、としている。他方、文民が敵対的行動を採った場合（「自身の敵対行為への直接参加」の場合）には、当該者はジュネーブ第1追加議定書50条3項に規定される「保護規定」の対象とならないとしている[30]。

他方、アメリカの国益を考えた研究者のあいだでは、アメリカ軍の指令系統の下で、市民がサイバー戦にかかわるオペレーションを行った場合、その人物は戦闘員と同じ保護規定が適用されるべきであるとの見方が最近出てきている[31]。

おわりに

本論文では、サイバー戦争が登場する前夜においても、武力行使が国連の安保理決議の採択を得つつ拡大する傾向があった点をまず指摘した。そのうえで、戦争のしかたが過去15年間、ハイブリッド戦争という通常戦とサイバー戦争の組み合わせによる戦闘に変化しつつあることを提示した。サイバー攻撃、サイバー戦争、さらにはサイバー行動などさまざまな用語が出現している現在、これまでの国際人道法や武力紛争法の規定や規範をサイバー戦争に適用するのは困難な点も本稿で明らかにした。サイバー戦争においては、文民と戦闘員の区別が曖昧になりがちであること、またサイバー攻撃がサイバー空間で引き起こされるため、国民国家の地理的主権が及ばない空間から攻撃を受け、攻撃者の特定がむずかしいこと、さらには、どのような基準をもって武力行使があったと認定するのか国際的な基準が定まっていないことなどを指摘した。

そうしたなか、この5年間のあいだ、武力紛争法のサイバー戦争への適用の国際的な規範づくりがさかんになった。武力紛争法の基礎づくりに貢献した赤十字国際委員会の立場は、武力行使の認定に対して慎重であり、サイバー攻撃や実害を及ぼすサイバー行動に対して予防の重要性を強調している。それに対し、NATOを中心とした規範づくりは赤十字国際委員会の立場とは反対に、サイバー行動の多くの側面をより積極的に武力行使とみなす傾向がある。しかしながら、あるサイバー行動を重大かつ深刻な平和への脅威だと被害国が決定したとしても、武力行為の責任がどの国家に帰属するのか（attribution）を正確に判定すること

が難しい以上、過剰な報復措置に至るリスクがある。また、あるサイバー行動がコンピュータ操作者の意図とは関係なく、深刻な被害を引き起こした場合、自分の意思とは関係なく「戦闘員」の資格を得る可能性がある。さらには、ある国家がサイバー攻撃を国家の安全保障にかかわるインフラに対して「深刻で重大な国家安全保障上の被害」を受けたと認定した場合、その効果に荷担した人物がいかなる国家の命令もなく、結果的にサイバー攻撃なる実態を引きおこした場合、その人物は文民なのか、戦闘員になるかなど、国際法上の問題は山積している。

兵役拒否の思想は、国家が殺戮や虐殺を引き起こす暴力装置になりうる状況下、いかにしてそれに荷担しないように兵役制度に抗うかという、平和思想として根源的な思想である。サイバー戦争が安価な戦争の一形態として頻発することが今後も見込まれる現在、兵役の担い手がサイバー攻撃に国家の指揮のもとに組み込まれるリスクは、従来型の通常戦より高い。なぜなら、サイバー攻撃を結果として引き起こすコンピュータ上の操作にどのような経路で誰が関与しているのか、末端のコンピュータ技師にはわからないからである。であるならば、兵役を担う者であるかどうかにかかわらず、一般市民が本人の意思とは無関係にサイバー戦争の攻撃者の一翼を担ったり、逆に無人飛行機の空爆を無差別的に受けたりする可能性もまた否定できない。

NATO を中心とするサイバー行動における武力行使の規範化が今後進展した場合、国家が安易に敵対国のサイバー行動を「武力」と認定し、報復行動に出るリスクは高まりつつある。たとえばロシアがウクライナをめぐり現在世界で展開しているサイバー攻撃に対し、武力行使だとアメリカが決定し、NATO 加盟国が報復戦争に動員された場合、加盟国の国民はサイバー戦という目に見えない戦争の渦中で戦時体制の下で生きることになる。暴力装置になりうる国家の権力に対し、今後個人はどのように抵抗し、暴力や武力行使に荷担することのないように身を守っていくのだろうか。エキュメニズム思想とその運動の根底にある、人間の尊厳を尊重する価値は今こそ重要な時代に入っている。国民国家における兵役拒否という枠組みを超え、兵役に無関係に生活していると考えがちな一般市民のあいだにも、そうした価値がより多く共有されることがこれまで以上に求められているのではないだろうか。

〈註〉

1) Marc Weller, *The Oxford Handbook of the Use of Force in International Law.* 2015, Oxford

University Press.

2) 芹田健太郎『国際人権法』（2018年）信山社、87頁。

3) Oliver P. Richmond (2004) "UN peace operations and the dilemmas of the peacebuilding consensus," *International Peacekeeping* 11:1 (2004): 93.

4) 松井芳郎『武力行使禁止原則の歴史と現状』（2018年）日本評論社、266頁。

5) Alan J. Kuperman, "A Model Humanitarian Intervention? Reassessing NATO's Libya Campaign," *International Security* 38-1 (2013): 105-136.

6) Graham Cronogue, "Responsibility to Protect: Syria, The Law, Politics, and Future of Humanitarian Intervention in Post-Libya," *International Humanitarian Legal Studies* 3 (2012): 124-159.

7) 松井芳郎、2018年、162-163頁。

8) Oona A. Hathaway, Rebecca Crootof, William Perdue, and Philip Levitz, The Law of Cyber-Attack, *California Law Review* 100-4 (2012): 826.

9) Kaniz Fatima; Sami Ur Rahman, "Cyber Warfare and Current Legal Regime: An Analysis of the Combatant Status and Principle of Distinction," Journal of Law and Society (University of Peshawar) 51 (2020): 71.

10) Kinetic という用語がこれに当たる。

11) Vivek Sehrawat, "Legal Status of Drones under LOAC and International Law," *Penn State Journal of Law and International Affairs* 5, no. 1 (April 2017): 182.

12) James T. Catania, Iran's Nuclear Program: A Presaging the Coming U.S. and Israeli Response (Navarre, FL: American Military University, 2011), 22–35; Brian P. Burrow, Engaging the Nation's Critical Infrastructure Sector to Deter Cyber Threats (Carlisle, PA: US Army War College, 2013), 13–14; Stimmel, 'Emerging Security and Data Privacy Challenges for Utilities,' 35.

13) James P. Farwell & Rafal Rohozinski (2011) "Stuxnet and the Future of Cyber War, " *Survival*, 53:1, 23-40. (https://doi.org/10.1080/00396338.2011.555586, 2022年1月4日取得)。,

14) 塩原、2015年、33頁。Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (2010) New York: HaperCollins Publishers.

15) Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars.* Arlington, VA: PIPS.

16) Greg Simons, Yuriy Danyk & Tamara Maliarchuk (2020) Hybrid war and cyberattacks: creating legal and operational dilemmas, *Global Change, Peace & Security*, 32:3, 337-342, p.339. (https://doi.org/10.1080/14781158.2020.1732899, 2022年1月5日取得)。

17) Chiyuki Aoi, Madoka Futamura & Alessio Patalano (2018) "Introduction 'hybrid warfare in Asia: its meaning and shape," *Pacific Review* 31-6: 706; Schmid, J. (2019b): 'The hybrid face of warfare in the 21st century'. Maanpuolustus, 127, 8 March 2019, Helsinki (FIN). (https://www.maanpuolustus-lehti.fi/the-hybrid-face-of-warfare-in-the-21st-century/ , 2021年12月24日取得)。

18) 一方で、サイバー戦争という用語ではなく、「サイバー行動」という新たな用語を登場させつつ、「武力行使」と同等の扱いをする傾向が強くなっている点は看過できない。

19) Sascha-Dominik Bachmann, "The Hybrid Wars: THE 21st CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY," Scientia Militaria, *South African Journal of Military*

Studies, Vol 43, No. 1 (2015): 82. 8

[20] 廣瀬陽子『ハイブリッド戦争―ロシアの新しい国家戦略』（2021）講談社、80-92 頁。ウクライナの事例については、次を参照。Piret Pernik, Chapter 5 The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine, HACKS, LEAKS, AND DISRUPTIONS Russia's Cyber Strategies (2018) European Union Institute for Security Studies. （https://www.jstor.org/stable/resrep21140.9, 2022 年 1 月 20 日取得）。

[21] Eric Luiiif and Kim Besseling, "Nineteen national cyber security strategies,"*International Journal of Cyber Security Strategies* 9-1/2 (January 2013):5-6.

[22] Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, 5, no. 4 (2011), p. 19.

[23] 塩原俊彦「サイバー空間と国家主権」『境界研究』No. 5（2015）pp. 29-56, p.34. 47. (http://hdl.handle.net/2115/61163、2021 年 10 月 2 日取得)。

[24] 鳥居 真由子「サイバー攻撃の武力紛争法上の課題」『エア・アンド・スペース・パワー研究』第 7 号　2021 年 3 月 31 日 107-110 頁。
（https://www.mod.go.jp/asdf/meguro/center/asp07.html, 2021 年 9 月 21 日取得）

[25] サイバー行動 (cyber operation) という用語は、正確には cyberspace operation のことを指しており、「サイバー空間において目的を達成するためことを主たる目的としてサイバー能力（cyber capabilities）を発揮することであり、コンピュータネットワークに関する操作（行動）やグローバルな情報グリッドを操作したり、防衛したりする活動を含む」と定義されている（Department of Dictionary of Military and Associated Terms, 2010, p.58,
https://irp.fas.org/doddir/dod/jp1_02.pdf.,2021 年 1 月 21 日取得）。
サイバー空間上のあらゆる活動や行動を包括的に捉えた用語として使用されている。

[26] ICRC（International Committee of Red Cross）*International Humanitarian Law and Cyber Operations during Armed Conflicts ICRC Position Paper* 2019.

[27] サイバー攻撃という用語を避けた表現となっており、これはサイバー的「武力」だと捉えた考え方になっている。

[28] Michael N. Schmitt. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, 2017, xii. (https://doi.org/10.1017/9781316822524, 2021 年 11 月 5 日取得)

[29] 中谷和弘・河野佳子・黒崎将広『サイバー攻撃の国際法―タリン・マニュアル 2.0 の解説』信山社、112 頁。

[30] 同上、108 頁。

[31] Christopher E. Bailey, "Cyber Civilians as Combatants," *Creighton International and Comparative Law Journal* 8, no. 1 (December 2016): 5.