【研究ノート】

サイバー攻撃の武力紛争法上の課題

航空研究センター防衛戦略研究室
2 等空佐　鳥居 真由子

はじめに

防衛省・自衛隊は現在、我が国に対する武力攻撃に伴い相手方がサイバー空間を利用することを妨げることができるよう能力の強化を図っている[1]。いわゆるサイバー攻撃[2]を含むこのような能力の使用は、防衛出動が下令され武力の行使が認められる場合には、自衛のための必要最小限度の範囲として認められる限り憲法上否定されないと考えられている[3]。ただし、武力の行使に関しては憲法上の制約が課されるだけではなく、国際法を遵守することも義務付けられている[4]。このため、自衛隊がサイバー攻撃を武力の行使の一環として行う上で、サイバー攻撃にいかなる国際法が適用されるのかを知ることは重要である。

国際法は、条約と慣習国際法からなるが、サイバー攻撃を特別に取り扱う条約はほとんど存在せず、締結されたわずかな条約の適用範囲も限定的である[5]。また、サイバーオペレーションに関する国家実行は軍や情報機関が行う場合が多いことから秘密であることが多く、国家がサイバーオペレーションに関してどのような国際法上の義務があると考えているのかということも公に表明されることが少ない。このため、サイバー攻撃に固有の慣習国際法を特定することは難しい状況にある。しかしながら多くの国家や国際法専門家の間では、既存の国際法はサイバーオペレーションに対しても適用可能であるという見解が広く共有されている[6]。

武力紛争中の敵対行為の規律の中心をなす武力紛争法（戦争法または国際人道法とも呼ばれる。）に関しても、通説は、全ての軍事行動に適用可能であり、

たとえサイバー空間を通じて行われる場合であっても例外ではないとする[7]。その一方で、後述するように、サイバー攻撃に対する武力紛争法の適用可能性に否定的な国家も少数ながら存在する。このため、サイバー攻撃に対して武力紛争法が適用可能であるという解釈が国際社会の共通理解として確立するか否かはっきりしないのも事実である。さらに、サイバー攻撃に武力紛争法が適用され得るという通説に立っても、その具体的な規則の内容については、国際法専門家の間でも未だ定まっているとはいえない。サイバー攻撃に関して今後自衛隊が検討を行う前提として、武力紛争法の解釈適用上の論点を整理しておく必要があるのはこうした理由による。

サイバー攻撃に関する武力紛争法の議論は、現在、国連総会決議に基づく政府間プロセス（政府専門家会合およびオープンエンド作業部会）を中心において行われている。また、このほかにも国際人道法の発展を促進するという観点から検討を行う赤十字国際委員会、さらに国際法学者間の学術的な議論も並行して進められている。そこで本研究では、これら三つの議論の場の特徴と性格、さらにそこで提起された議論を確認した後、サイバー攻撃に関する武力紛争法上の論点整理を通じて、武力攻撃事態におけるサイバー戦について自衛隊が今後検討すべき事項を明らかにすることとする。

１　国際的な議論の状況

(1)　国連総会決議に基づく政府間プロセス

サイバーセキュリティは、1998 年以来、国連の議題の一つとなってきた[8]。この問題を話し合う場として最も重要な場が、2004 年以降国連総会決議に基づいて設置された政府専門家会合と 2018 年に設置されたオープンエンド作業部会である[9]。

ア　政府専門家会合

サイバーセキュリティに関する政府専門家会合は、これまで、6 回の会合が設定され、サイバー空間における現在および将来の脅威とこれらの問題に対処するための協力措置について検討が行われてきた[10]。第 6 回の政府専門家会合は、2019 年から開催されており、2021 年の国連総会に報告書を提出する予定である[11]。会合の構成は衡平な地理的配分を基礎としており、国連安保理常任理事国と、国連地域グループによってメンバーシップを割り当てられた国から構成される[12]。実際の構成国は、次の表のとおりである[13]。

政府専門家会合	構成国
第1回 （2004-2005）	ベラルーシ、ブラジル、中国、フランス、ドイツ、インド、ヨルダン、マレーシア、マリ、メキシコ、韓国、ロシア、南アフリカ、イギリス、アメリカ　（15か国）
第2回 （2009-2010）	ベラルーシ、ブラジル、中国、エストニア、フランス、ドイツ、インド、イスラエル、イタリア、カタール、韓国、ロシア、南アフリカ、イギリス、アメリカ　（15か国）
第3回 （2012-2013）	アルゼンチン、オーストラリア、ベラルーシ、カナダ、中国、エジプト、エストニア、フランス、ドイツ、インド、インドネシア、日本、ロシア、イギリス、アメリカ　（15か国）
第4回 （2014-2015）	ベラルーシ、ブラジル、中国、コロンビア、エジプト、エストニア、フランス、ドイツ、ガーナ、イスラエル、日本、ケニア、マレーシア、メキシコ、パキスタン、韓国、ロシア、スペイン、イギリス、アメリカ　（20か国）
第5回 （2016-2017）	オーストラリア、ボツワナ、ブラジル、カナダ、中国、キューバ、エジプト、エストニア、フィンランド、フランス、ドイツ、インド、インドネシア、日本、カザフスタン、ケニア、メキシコ、オランダ、韓国、ロシア、セネガル、セルビア、スイス、イギリス、アメリカ　（25か国）
第6回 （2019-2021）	オーストラリア、ブラジル、中国、エストニア、フランス、ドイツ、インド、インドネシア、日本、ヨルダン、カザフスタン、ケニア、モーリシャス、メキシコ、モロッコ、オランダ、ノルウェー、ルーマニア、ロシア、シンガポール、南アフリカ、スイス、イギリス、アメリカ、ウルグアイ　（25か国）

政府専門家会合は、検討を踏まえた報告書案を作成し、コンセンサスが得られた場合には報告書を国連事務総長に提出するが、そこに至る検討過程については明らかにされない。また、会合内で合意が形成されない場合には、参加者のリストと会合の日程のみを記載した報告書が提出される[14]。

政府専門家会合の参加者は多くの場合、政府職員である。初期の会合では、外交の専門家と科学技術系の専門家の混合であったが、次第に、各国は外交、軍備管理、不拡散の専門家を参加者として選出する方向に変わっていくとともに、法律顧問を同伴することが一般的となっている[15]。なお、率直な議論を行うため、後述するオープンエンド作業部会とは異なり、この政府専門家会合の内容は秘密とされ、国、NGO、民間セクター、国際組織を問わず、オブザーバー参加は認められていない[16]。

第3回政府専門家会合（2012年～2013年）では、国際法はサイバー空間に適用

可能であるという合意が初めてなされたものの[17]、この時の報告書においては、武力紛争法の適用可能性に関する明言はなされなかった。このため、サイバー空間における国家の行動に武力紛争法が適用されるべきと当時の各国政府の専門家が考えていたかどうかは定かではない。その後、第4回政府専門家会合（2014年～2015年）で、各国政府の専門家は、国際法がサイバー空間に適用可能であることを再度確認するとともに、国家がサイバー空間で行動するに当たって国際法がどのように適用されるのかという問題を検討した[18]。この際、サイバー空間への武力紛争法の適用については、中国を含む多くの国が反対したため、同会合の報告書は、人道性、必要性、比例性、区別という武力紛争法の主要な原則に言及する一方、そのサイバー空間への適用について明確な認識を示すことはできなかった[19]。第5回政府専門家会合（2016年～2017年）においてもサイバー空間への武力紛争法の適用可能性について検討が行われたが、キューバ、ロシア、中国等の反対があり、コンセンサスを得るには至らなかった[20]。

武力紛争法の適用可能性に否定的な立場をとる理由は明らかではないが、キューバおよび中国は、サイバー空間への武力紛争法の適用を認めることでサイバー行動やサイバー戦争を正当化することとなるのではないかとの懸念を抱いているとされている[21]。加えて中国は、サイバー空間において民用物と軍事目標とを区別することが不可能であるとして、武力紛争法の適用可能性の問題以前にサイバー戦争それ自体を予防することに重きを置くべきとの立場をとっている[22]。

しかしながら、このような反対国の主張は、長年受け入れられてきた武力紛争法の解釈と三つの点で一致しない。まず第一に、武力紛争法は、戦争のやり方を規律する法である。したがって、サイバー戦争の予防についてはむしろ戦争の正当化理由を規律する武力行使法（*jus ad bellum*）と呼ばれる別の国際法分野が規律する問題であるといえる。つまり、武力紛争法をサイバー戦に適用できるか否かという問題と、サイバー空間の軍事化やサイバー戦争の予防とは切り離して考えられるべきである[23]。第二に、武力紛争法の諸原則は、過去、現在、未来を問わずあらゆる形態の戦闘とあらゆる種類の武器に適用可能であると考えられてきた[24]。つまり、サイバー戦が新たな戦い方であることは、武力紛争法の適用可能性を排除する理由にはならない。第三に、現実世界において戦争を予防することと事実として発生した武力紛争に対して武力紛争法を適用することが両立するように、サイバー戦争を予防することとサイバー戦に武力紛争法を適用することは何ら矛盾しない。しかも、ある戦闘の手段と方法が武力

紛争法に一致しない場合には、当該手段と方法は武力紛争法上違法となるだけであり、武力紛争法全体の適用可能性を排除するということにはならない。つまり、もしサイバー空間において民用物と軍事目標とを区別することが不可能であるとしても、そのことはサイバー空間に武力紛争法全体が適用されない理由にはならないのである[25]。

サイバー空間への武力紛争法の適用可能性に否定的な反対国の主張の裏には、科学技術の発展を見極めてから法を明確にしたいという考えや、法をあいまいなままにして行動の自由を残そうとする戦略的な思惑があるとみられている[26]。

イ　オープンエンド作業部会

オープンエンド作業部会は、「国際安全保障の観点から見た情報通信分野の発展」と題した2018年12月5日の国連総会決議73/27によって、閉鎖的な政府専門家会合とは対照的に、全国連加盟国、国際機関およびNGO等にも広く参加が開放される形で設置された。同作業部会は、第6回政府専門家会合と並行して2019年から開催され、2020年国連総会への報告書提出を目指して検討を進めていたが[27]、新型コロナウイルスのパンデミックに伴いスケジュールが見直され、報告書の提出時期も第76回の国連総会（2021年）へと延期される方向にある[28]。

同作業部会は、第3回および第4回政府専門家会合において認められた国際法の規則および原則をさらに発展させることを検討事項の一つとしており[29]、武力紛争法の適用に関しても意見交換を行っている[30]。

武力紛争法の適用を認める国	武力紛争法の適用自体に否定的な国
アルゼンチン、オーストラリア、オーストリア、ブラジル、チリ、コロンビア、チェコ、デンマーク、エジプト、エストニア、フランス、ドイツ、アイルランド、イタリア、日本、ルクセンブルク、オランダ、パキスタン、スウェーデン、スイス、英国、米国、ウルグアイ、ジンバブエ、上記以外のEU加盟国	キューバ、中国、インドネシア、イラン、ニカラグア、ロシア、ベネズエラ

現在、作業部会は、報告書第2次仮草案（2020年5月27日時点）において、「特に国際連合憲章全体を含む国際法上の既存の義務は、国家による情報通信技術の使用に対して適用可能」[31]であることを再確認している。その上で、「国際人道法は武力紛争中の文民および戦闘員へのリスクおよび潜在的な危害を低減

する」[32]と評価し、「諸国は、いかなるドメインにおいても国際人道法が軍事化を促進することも、紛争に訴えることを合法化することもないと強調した」[33]と述べている。他方、「国家の情報通信技術の使用に対する国際人道法の適用可能性に関しては慎重に議論する必要があることに留意すべきである」[34]と武力紛争法の適用可能性に否定的な国に対する配慮を見せており、今後、武力紛争法そのものの適用可能性については引き続きあいまいさが残る可能性がある。

(2)　赤十字国際委員会

赤十字国際委員会は、国際人道法の発展に貢献することを任務の一つとしており[35]、2003年以降、4年ごとに行われる赤十字・赤新月国際会議[36]に対して「国際人道法と現代の武力紛争の課題」と題する報告書を繰り返し提出してきた。この報告書の目的は、現代の武力紛争が国際人道法にもたらす課題の概要を示して問題提起するとともに、現在および将来の赤十字国際委員会の関心、立場、行動を説明することにある[37]。サイバー戦は、2011年以降継続して、この報告書のトピックの一つとなっている[38]。以下では、主に2019年の報告書に基づき、サイバー戦に関する赤十字国際委員会の認識を整理していくこととする[39]。

まず、赤十字国際委員会は、サイバー空間に武力紛争法が適用可能であるとの立場をとっている[40]。ただし、武力紛争法がこれまでサイバー戦を想定していなかったため、武力紛争中に行われるサイバー戦に対して武力紛争法がどのように適用されるのかということは明らかではなく、また、サイバー攻撃には他の戦闘の手段・方法とは異なる特有のリスクがあると解している[41]。そこで赤十字国際委員会は、武力紛争法が軍事行動の影響からの文民たる住民の保護を主要な目的の一つとしているということに鑑みて、サイバー戦が文民に与える影響を出発点として、次のとおり検討した。

産業部門ごとに検討した結果、文民に与える影響が特に大きいのは、医療および重要民生インフラ（電気、水、衛生施設を含む。）である。特に医療では、デジタル化と相互接続性の向上により、病院内の医療機器に加えてペースメーカーやインスリンポンプといった生体医療機器もリモートで病院のネットワークへ接続しており、サイバー攻撃にさらされている部分が広い。このため、医療部門は、直接的なサイバー攻撃にも別の場所で発生したサイバー攻撃の余波にも脆弱である[42]。

また、どのサイバー攻撃であっても共通する問題として、少なくとも次の三つの懸念が指摘されている。第一の懸念は、過剰反応やエスカレーションの危

険である。サイバー攻撃は、諜報活動の目的でも物理的破壊を引き起こす目的でも行われる可能性があるが、ターゲット側がその目的を知ることは困難である。このため、ターゲット側が最悪のケースを想定して過剰反応をするおそれがある[43]。第二の懸念は、サイバーの手段・方法の拡散の危険である。洗練されたサイバー攻撃を行うには、最先端の技術と大きな資金力が必要とされるが、サイバーの手段・方法がいったん使用されたり盗まれたり漏洩する等の何らかの事情で利用可能な状態になってしまえば、解析調査されて他者に悪用される可能性がある[44]。第三の懸念は、サイバー攻撃の実行者の特定が困難な傾向にあることである（アトリビューション問題）。サイバー空間において武力紛争法違反者を特定し責任を負わせることは引き続き難しいことが見込まれるが、それにより当該責任追及の意味がなくなるということになれば、サイバー空間における武力紛争法遵守の可能性もそれだけ低くなってしまう[45]。

以上の問題を踏まえたうえで、赤十字国際委員会は、このようなサイバー攻撃の影響に対して武力紛争法が与える保護について、武力紛争法の一般原則[46]、特別の保護対象[47]、区別原則[48]、比例性原則[49]、攻撃側の予防原則[50]、防御側の予防原則[51]、文民たる住民に対する一般的保護[52]の観点から、次のように述べている[53]。

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。

赤十字国際委員会の見解において注目すべき点は、データの位置付けをめぐる考え方である。これは、既存の武力紛争法規則の解釈に一石を投じるものである。

武力紛争法には、民用データの消去または改ざんなどのサイバー攻撃を直接的かつ明示的に規律する条約規則も慣習法規則も存在しない。しかし、このことは、サイバー攻撃に関する武力紛争法の欠缺（けんけつ）（規律する法規則が存在しないこと）を意味するものではない。既存の武力紛争法規則を解釈し適用することでこの問題にアプローチすることは十分に可能だからである。もっとも、具体的にどのような武力紛争法規則がここで問題となっているかについては争いがある。主たる争点は、特に攻撃に関する区別原則（軍事目標主義）の適用可能性である。

区別原則は、特に攻撃対象を軍事目標に限定し文民と民用物の保護を紛争当事者に求めるものであるが、デジタル・データが軍事目標（military objectives）になるのか、または非攻撃対象として保護されるのかどうかについては、後述するように、専門家の意見が一致していない[54]。この点について、国際法学者の多数派は、対象が「物（object）」であることが前提条件となるが、データはそのような性格を有していないと考えている[55]。これはつまり、データが法的に「物」であると評価できない限り、これを軍事目標と非軍事目標のいずれにも評価できず、結果として、攻撃に関する既存の武力紛争法の枠組ではデータの消去または改ざんのみを目的とするサイバー攻撃を規律できないということを意味する。実際、タリン・マニュアルの責任者であるマイケル・シュミット（Michael Schmitt）は、データを「物」と評価することはできず、データの消去

または改ざんのみを目的とするサイバー攻撃に対して武力紛争法上の攻撃の規則を適用することについては立法論にならざるを得ないと主張している[56]。

他方、もし、このようなサイバー攻撃が攻撃よりも広い概念である「軍事行動」に包含される場合には、文民はそうした行為から生ずる危険からの一般的保護を受けることができる可能性がある[57]。しかし、この場合、具体的にどのような保護が与えられるのかにつき、その内容は、明らかではない。

なお、赤十字国際委員会が、果たして、①データを「物」と評価し攻撃に関する既存の武力紛争法の規則が適用されるものと解釈しているのか、あるいは、②攻撃に関する既存の武力紛争法の枠組上、データを「物」として評価していないものの、立法論としてそのような解釈の必要性を主張しているのか、はたまた、③軍事行動から生ずる危険からの一般的保護の規則を具体化することで保護を図ろうとしているのかは、明らかではない。しかしながら、同委員会の立場がいずれであったとしてもデータの消去または改ざんをめぐる武力紛争法規則がこのように国際法専門家の間で論争を呼ぶ問題となっているということには、留意する必要があるだろう。

(3)　国際法学者間の議論

文民の保護は武力紛争法の目的の一つであることから、サイバー戦に関する現行法解釈に関して国際法学者の間で交わされている議論においても、重要な民生インフラおよび民用データをサイバー攻撃から保護することは重要な論点となっている。区別原則、比例原則、予防原則など、多くの規則が攻撃をめぐって規定されているように、武力紛争法は、攻撃という概念を中心に敵対行為を規律している。したがって、この論点についても、①サイバー攻撃を武力紛争法上の攻撃の概念に含めることができるのか、および②データを武力紛争法上の攻撃対象、あるいは保護対象と認めることができるのか、に焦点を当てて検討がなされてきた。

ア　サイバー攻撃はどこから武力紛争法上の攻撃となるか

攻撃の定義について、1949年ジュネーヴ諸条約第1追加議定書（1977年）（以下、本文においては「第1追加議定書」とする。）は、「攻勢としてであるか防御としてであるかを問わず、敵に対する暴力行為をいう」と規定している[58]。そして、この「暴力行為」は、キネティックな力を放出する活動に限定されないと解されている。例えば、非キネティックな化学攻撃、生物攻撃、放射能攻撃が武力紛争法上の攻撃とされてきたように、攻撃という概念の核心は、引き起こされる暴力的な効果にあるとされている[59]。

他方、どのような効果があれば攻撃となるのかについては、議論がある。タリン・マニュアルは、比例原則および攻撃の際の予防措置の規定において、攻撃の付随的な効果として文民の死傷と民用物の損傷・破壊が列挙されていることに注目した[60]。そして、武力紛争法上の攻撃となるサイバー攻撃を「攻勢としてであるか防御としてであるかを問わず、人に対する傷害若しくは死、または対象に対する損傷若しくは破壊を引き起こすことが合理的に予期されるサイバー行動」[61]とした（危害説）。危害説は、第1追加議定書上の攻撃の定義から容易に導くことができる一方で、危害を引き起こさない多くのサイバー攻撃を武力紛争法上の攻撃から排除してしまうことで文民および文民たる住民の法的保護が脆弱となることが問題視されている。例えば、送電網システムに介入して大規模停電を引き起こすサイバー攻撃は、武力紛争法上の攻撃に当たらないこととなり、それに対する被害が文民に及んでも直ちに違法にはならない可能性も出てきてしまう[62]。

こうした危害説の短所を克服する形で少数の国際法学者によって提起されているのが、手段を問わず、対象を無効化することを攻撃と位置付ける説である（無効化説）[63]。この説によれば、無効化の方法は、キネティックな手段によるものであろうと、サイバー攻撃であろうとかまわないため、対象の損傷・破壊を伴わないサイバー攻撃を武力紛争法上の攻撃に包含することが可能となる。この説は、合法な攻撃目標を定める軍事目標の定義において、攻撃の結果として物の破壊と無効化が並列に列挙されていることに着目したものである[64]。ただし、無効化説にも課題があり、オンライン・ショッピング・サービスや旅行代理店等へのDoS攻撃をも包含してしまう。このため、無効化説は、攻撃の定義として広すぎるということが指摘されている[65]。

以上、サイバー攻撃はどこまで武力紛争法上の攻撃なのかという観点から、攻撃の定義を巡る議論を概観したが、論争はいまなお決着していない。

イ　データは「物」か

この議論では、サイバー攻撃のうち、特にデータの消去または改ざんするものに焦点が当てられている。現時点において、武力紛争中に民用データをサイバー攻撃から保護する特別の規定はないが、もし民用データそのものが武力紛争法上の民用物であれば、区別原則により損傷・破壊（消去または改ざん）から保護されることとなる。さらに比例原則により、民用データに対して過度の付随的損害を与えることも禁止される。民用データが武力紛争法上の民用物と判断できる場合、文民の生活にとって重要な民用データに対してこうした保護

が与えられることとなる。

第1追加議定書は、民用物について、軍事目標以外の「すべての物（object）」と規定しており、軍事目標について、「物（object）については、その性質、位置、用途または使用が軍事活動に効果的に資する物であってその全面的または部分的な破壊、奪取または無効化がその時点における状況において明確な軍事的利益をもたらすものに限る」と定義している[66]。ここから分かるように、民用物および軍事目標は、まず「物（object）」であることを前提としている。

国際法学者の多数派は、第1追加議定書のコメンタリーがこの「物」とは「見て触ることができる」ものであると解説していることから、データを物とみなすことはできないと解釈した（データ非物体説）[67]。これに対して民用データの保護の必要性を重視する国際法学者らは、「物」にはデータも含まれると主張している（データ物体説）[68]。データ物体説をとる国際法学者は、自説の補強のため、第1追加議定書が「物」という言葉を使用することで軍事目標や民用物の議論から排除しようとしたのは何かという点に注目した。その結果、同議定書が排除しようとしたのは、「文民の士気」のような抽象的な概念であると考えられた。また、コメンタリーが「物」を「見て触ることができる」ものと解説した趣旨も、“object”の意味から「目的または目標」という抽象的な意味を排除しようとしたものであると考えられた[69]。データ物体説の論者は、こうした事情も併せて、重要な民用データを保護するために「物」の意味を拡大してデータを包含することを主張している。

重要な民用データがサイバー攻撃を受けた場合の影響の大きさから、データ非物体説の立場に立つ論者も、自説の課題を認識している[70]。その一方で、データ物体説についても、それを支持する国家実行や法的確信がないことから現行法解釈ではなく立法論であるとの批判が根強い[71]。このため、当該議論についても決着はついていない。なお、どちらの説をとるとしても、次のような問題が残るため、対策の具体化に向けた検討がさらに必要となるだろう[72]。

	問　　題
データ非物体説	【ケース】 戸籍、納税、年金、銀行口座等の電子データの改ざん又は破壊 【懸念】 このようなサイバー攻撃が行われれば、行政活動の中断や文民の生活の混乱が予想され、場合によっては、ミサイルや爆弾による民用物の直接破壊よりも深刻な文民への悪影響が生じ得る。 【武力紛争法上の評価】 当該サイバー攻撃は違法とは言えない。 ・データは物ではないため攻撃の規則によって規律できないから。 【対策】 紛争当事者が、ROE等を通じて、サイバー攻撃に対する政策上の制限を設ける。
データ物体説	【ケース】 軍隊によるWi-Fiやインターネット接続の使用 【懸念】 敵がネットワーク全体を軍事活動に効果的に資する軍事目標とみなし、次のような攻撃を行うことにより、デュアルユースのネットワーク全体が甚大な被害を受ける可能性がある。 ①当該ネットワークに対して、軍隊が使用する部分か否かを区別することなくサイバー攻撃を行う。 ②当該ネットワークを構成するサイバーインフラに対して、伝統的な兵器を用いた爆撃を行う。 【武力紛争法上の評価】 ①の攻撃の法的評価には争いがある。 ・当該ネットワークを単一の軍事目標とみなすことができる場合には、敵の攻撃は違法とは言えない。 ・ネットワーク内の敵軍隊のコードを識別可能な場合には、当該コードだけを攻撃目標としなければならず、ネットワーク全体への攻撃は違法である。 ②の攻撃は違法とは言えない。 ・当該ネットワークが軍事目標である以上、伝統的兵器を用いて爆撃することは違法ではない。 【対策】 サイバーターゲティングに関する武力紛争法解釈及び実行可能な措置の明確化

２　自衛隊が検討すべき課題

以上の国際的な議論を踏まえ、最後に、①サイバー空間への武力紛争法の適用可能性、②サイバー攻撃に適用可能な武力紛争法の解釈、および③武力紛争法遵守の観点から必要な施策の三つの側面から、今後自衛隊が検討すべき課題を整理する。

(1)　サイバー空間への武力紛争法の適用可能性について

まず、武力紛争の一環として行うサイバー攻撃に、武力紛争法は適用されるのであろうか。

我が国政府は、この問題について、「国際連合憲章および国際人道法を含む既存の国際法が、サイバー空間の使用に適用可能であると確信している」と述べている[73]。同様に、アルゼンチン、オーストラリア、ブラジル、カナダ、チリ、コロンビア、エジプト、パキスタン、スイス、英国、米国、ウルグアイ、ジンバブエ、およびEU加盟国もまた、さまざまな場所で武力紛争法のサイバー空間への適用を支持する見解を示している[74]。他方で、上述のように、サイバー政府専門家会合では、常時メンバーシップを割り当てられている国連安保理常任理事国のロシアおよび中国がサイバー空間への武力紛争法の適用に反対するなど、同会合ではサイバー空間への武力紛争法の適用可能性について合意が形成されていないのも事実である。オープンエンド作業部会でも中国およびロシアに加えて、キューバ、インドネシア、イラン、ニカラグア、ベネズエラがサイバー空間への武力紛争法の適用可能性に否定的な立場を表明している。以上のことに鑑みれば、政府専門家会合同様オープンエンド作業部会でも、国際社会の共通理解として武力紛争法がサイバー空間に対して適用可能であると明記される可能性はやはり低いものと思われる。

いずれにせよ日本としての公式見解が上述のとおりである以上、自衛隊としても、今後はサイバー空間への武力紛争法の適用を前提にサイバー戦の戦い方の検討および防衛力整備を進めるべきであると思料する。

(2)　サイバー攻撃に適用可能な武力紛争法の解釈

本研究で確認してきたとおり、サイバー攻撃に関する武力紛争法については、攻撃や物という極めて基本的な概念をめぐって論争が続いている。これは、従来の武力紛争法がサイバー戦を想定していなかったことに加え、社会のデジタル化が進み、サイバー攻撃が行政活動や経済活動を停止させるほどのインパクトを持ったことによるところが大きい。

こうした状況ゆえに、自衛隊がサイバー戦の戦い方を検討する際には、まず、

武力紛争法上の攻撃概念の射程および文民の生活における民生インフラや民用データの重要性を考慮した具体的な保護措置（政策的判断によるものを含む。）の必要性と可能性を整理する必要がある[75]。

(3)　武力紛争法遵守の観点から必要な施策

ア　サイバー攻撃の手段・方法の合法性審査

上述のように、サイバー空間への武力紛争法の適用を前提にすれば、ある種のサイバー攻撃は武力紛争法上の攻撃となり得る。一方、我が国が締約国となっている第1追加議定書第36条は、新たな戦闘の手段・方法の研究、開発、取得または採用に当たり、その使用が武力紛争法によって禁止されていないかを決定する義務を課している。このため、サイバー攻撃能力の整備に当たっても、合法性審査を実施することが必要であろう[76]。

イ　サイバー攻撃に適用可能な武力紛争法の教育

武力紛争法は、軍隊がその構成員に対して各人の責任に応じた内容を了知させるよう求めている[77]。このため、サイバー攻撃に適用可能な武力紛争法上の禁止、制限及び義務並びにそれらの具体的基準は、サイバー攻撃を計画し実行する指揮官、その幕僚および実際に攻撃を行う隊員ごとに必要な内容を精査し、それぞれの教育訓練に反映される必要であろう。

ウ　サイバー攻撃のターゲティング手続の検討

武力紛争法上、紛争当事者は、攻撃の計画および実施に際して、区別原則および比例原則を踏まえ、攻撃目標の選定、攻撃手段・方法の選定、付随的損害の予測および攻撃の影響を受ける文民への警告等を行う義務を負っている[79]。各国軍隊では、こうした武力紛争法上の義務を踏まえてターゲティングの手続を定めている[80]。他方、サイバー攻撃については、上述のように、全てが武力紛争法上の攻撃となるのか否か解釈が分かれている。このことを踏まえ、一部の国際法専門家は、サイバー攻撃に独自のターゲティング手続が必要となる可能性を指摘している[81]。いかなる手続が最適かを明らかにするためには、当該ターゲティング手続が適切かつ効果的な指揮活動および部隊運用に資するかどうかという観点とも両立するよう実際的な検討と検証を行っていくことが必要であろう。

おわりに

本研究は、武力紛争中の敵対行為の遂行を規律する武力紛争法に焦点を当て

て国際的な議論の動向を整理し、自衛隊がサイバー攻撃に関して今後検討すべき課題を考察した。

現在、サイバー空間への武力紛争法の適用について、国際社会の合意は形成されていないが、日本政府がこれを肯定している以上、自衛隊も同法の適用を前提にサイバー戦を検討する必要があるだろう。もっとも、サイバー攻撃に関する武力紛争法においては、どのようなサイバー攻撃から法上の攻撃に当たるか、また、データは物か否か、といった問題をはじめとする重要な難題が山積している。よって、サイバー戦の戦い方を検討する際には、まず、武力紛争法上の攻撃概念の射程および民生インフラや民用データに対する具体的な保護措置の必要性や可能性について考え方を整理していく必要がある。

---

[1] 防衛省『令和 2 年版防衛白書』2020 年、271 頁；「中期防衛力整備計画（平成 31 年度～平成 35 年度）について」平成 30 年 12 月 18 日国家安全保障会議決定・閣議決定、Ⅲ・1(1)(イ)。

[2] 『令和 2 年版防衛白書』は、サイバー攻撃として、情報通信ネットワークや情報システムなどの悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行や DDoS 攻撃（分散型サービス不能攻撃）などを挙げている。防衛省『令和 2 年版防衛白書』271 頁注 6。サイバー攻撃に適用可能な国際法を検討したタリン・マニュアル 2.0 は、サイバー攻撃を「攻勢としてであるか防御としてであるかを問わず、人に対する傷害若しくは死、または物に対する損害若しくは破壊を引き起こすことが合理的に予期されるサイバーオペレーション」と定義し、武力紛争法上の攻撃の定義（1949 年ジュネーヴ諸条約第 1 追加議定書（1977 年）（以下、脚注においては「API」とする。）第 49 条第 1 項）と平仄を合わせている。これに対して、赤十字国際委員会は、サイバー攻撃を「アクセスを獲得し、データを抜き取り、かつ（または）データ若しくはサービスを暗号化し、劣化させ、変更若しくは無効にするため、ターゲットとなるシステムの所有者の同意を得ずに、またはその所有者が認識していないところで実行されるあらゆるサイバーオペレーション」を指すものと定義している。これは、物に対する物理的な損害または破壊に攻撃の定義を限定しない点で、API に基づくタリン・マニュアル 2.0 よりも広い概念整理を行ったものと見ることができる。このような定義を同委員会が採用したのは、後述するように武力紛争の一環として民用データ（社会保障番号、納税記録、預金口座、顧客ファイルまたは選挙リスト・記録）を消去または改ざんして、政府の業務や私企業のビジネスの完全な停止、その他、文民にとって物を物理的に破壊されるよりも有害な結果を引き起こすような敵対行為をも武力紛争法は規制すべきであるとの立場を取っているためであろう。本稿は、タリン・マニュアルだけでなく、サイバー攻撃に関する武力紛争法上のさまざまな見解を整理することを目的とするものであるため、サイバー攻撃を広く捉える赤十字国際委員会の理解に沿って検討を進めている。Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the international Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p. 415 (Rule 92) [hereinafter *Tallinn Manual 2.0*]; *The Potential Human Cost of Cyber Operations, ICRC Expert Meeting 14-16 November 2018*, ICRC, May 2019, p. 11, https://www.icrc.org/en/publication/potential-human-cost-cyber-operations; International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary armed Conflicts*, 32nd

International Conference of the Red Cross and Red Crescent 8-10 December 2015, October 2015, p. 43 [hereinafter *ICRC IHL Challenges Report 2015*]. なお、*Tallinn Manual 2.0* をコンパクトに解説したものとして、中谷和弘、河野桂子、黒﨑将広『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、2018 年がある。

[3] 「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」。第 201 回国会衆議院安全保障委員会議録第 4 号、令和 2 年 4 月 7 日、13 頁、河野太郎防衛大臣答弁；「サイバー攻撃を伴い、さらに、それと同時に実際の武力行使、武力による攻撃があった場合、これは武力行使の三要件を満たすという判断があった場合には、内閣総理大臣は、自衛隊法第 76 条 1 項の規定に基づき防衛出動を下令することができ、そして、同法 88 条 1 項において、76 条 1 項の規定により出動を命ぜられた自衛隊は、我が国を防衛するために必要な武力を行使することができるという規定があります。この必要な武力を行使するとの具体的な内容については、当該事態の態様や状況によって異なり、一概に述べることは困難でありますが、法理的には、この必要な武力を行使することの一環として、いわゆるサイバー攻撃という手段を我が国が用いることは否定されないと考えております」。第 196 回国会衆議院安全保障委員会議録第 3 号、平成 30 年 3 月 22 日、7 頁、小野寺五典防衛大臣答弁；第 197 回国会衆議院内閣委員会議録第 6 号、平成 30 年 11 月 22 日、3 頁、小波功防衛省大臣官房サイバーセキュリティ・情報化審議官答弁。

[4] 自衛隊法第 88 条。

[5] 例えば、欧州評議会を中心として成立したサイバー犯罪に関する条約（2001 年署名、2004 年効力発生）は、インターネットその他のコンピュータ・ネットワークを通じて実行される犯罪に関する最初の国際条約であり、特に、国内立法及び国際協力を助長することにより、サイバー犯罪から社会を守ることを目的とした共通の刑事政策を追求することを主たる目的としている。著作権の侵害、コンピュータ関連詐欺、児童ポルノ及びネットワーク・セキュリティの侵害について取り扱っており、違法なアクセス、違法な傍受、データの妨害、システムの妨害、装置の濫用、コンピュータに関連する偽造、コンピュータに関連する詐欺等について国内法によって犯罪化することを求めている。また、コンピュータ・ネットワークの捜査や傍受のような権限及び手続についても規定している。ブダペスト条約ともいう。2020 年 8 月 19 日時点の締約国は、65 か国。日本は、2012 年にこの条約の締約国となった。アイルランド、ロシア、スウェーデンについては、欧州評議会の構成国であるが、この条約の締約国ではない。欧州評議会構成国以外の締約国には、日本のほか、オーストラリア、カナダ、イスラエル、フィリピン、米国等がある。他方、中国、インド、北朝鮮、韓国はこの条約の締約国ではない。“Details of Treaty No.185: Convention on Cybercrime,” Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[6] *Tallinn Manual 2.0*, pp. 3-4.

[7] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I. C.J. Reports 226, 1996*, para. 86; Advisory Committee on Issues of Public International Law, *Cyber Warfare*, No. 77, AIV/No. 22, CAVV, December 2012, p. 24; *ICRC IHL Challenges Report 2015*, p. 40; “The Oxford Statement on the International Law Protections against Cyber Operations targeting the Health Care Sector,” Oxford Institute for Ethics, Law and Armed Conflict, https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea. なお今日、武力紛争中の行為には国際人権法等、武力紛争法以外の国際法も適用されるものの、主に規律しているのは武力紛争法である。Department of Defense, Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated December 2016), pp. 9-10 [hereinafter *US DoD Law of War Manual*]; Advisory Committee on Issues of Public International Law, *Cyber Warfare*, p. 24; Kubo Mačák, “From Vanishing Point Back to the Core: the Impact of the Development of the Cyber Law of War on General International Law,” 2017 9th International Conference on Cyber Conflict, NATO CCDCOE Publication, 2017, pp. 3-4.

[8] United Nations General Assembly, *Resolution Adopted by the General Assembly 53/70. Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Document A/RES/53/70, January 4, 1999. 1998 年にロシアがサイバーセキュリティを国連総会第 1 委員会の議題とすることを提案し、そのとおり国連総会で採択された。政府専門家会合が開催されたのは 2004 年以降であるが、サイバーセキュリティに関する国連加盟国の見解を求める決議は 1999 年から例年出されている。“Fact Sheet Development in the Field of Information and Telecommunications in the Context of International Security,” United Nations Office for Disarmament Affairs, July 2019 [hereinafter “Information Security Fact Sheet 2019”], https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

[9] 国連安全保障理事会においては、これまでサイバーの脅威をテーマとする公式会合が開かれたことはないが、アリア・フォーミュラ会合という非公式な枠組では議論されてきた。2016 年 11 月 28 日におけるサイバーセキュリティと国際の平和および安全に関するアリア・フォーミュラ会合、2016 年 11 月 21 日におけるテロ攻撃に対する重要インフラ防護に関するアリア・フォーミュラ会合、2017 年 3 月 31 日における国際の平和および安全に対する脅威としてのハイブリッド戦に関するアリア・フォーミュラ会合、そして 2020 年 5 月 22 日におけるサイバーの安定性、紛争予防および能力構築に関するアリア・フォーミュラ会合がこれまで開催されている。“Arria-formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building,” What’s in Blue, May 21, 2020, https://www.whatsinblue.org/2020/05/arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building.php; Maria Tolppa, “International Cyber Stability Framework at the United Nations Security Council,” CCDCOE, https://ccdcoe.org/libtary/publications/international-cyber-stability-framework-at-the-united-nations-security-council/; “Signature Event of Estonia’s UNSC Presidency: Cyber Stability, Conflict Prevention and Capacity Building,” Ministry of Foreign Affairs, Republic of Estonia, June 29, 2020, https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber. なお、2020 年 5 月 22 日の会合では、ロシアのみ不参加であったが、同国はプレスリリースにて、次の通りサイバー空間に対する国際人道法の適用可能性に否定的な立場を表明している。「少数のエリート国が、『予防的軍事サイバー攻撃』（重要インフラを対象とする攻撃を含む。）という概念を推し進めることにより、積極的にサイバー空間の軍事化を追求していることは、重大な懸念である。特定の国々が、他の国連加盟国に対する一方的な圧力および制裁ならびにそれらの国に対して行う可能性のある武力行使を正当化するために、情報空間に対して国際人道法を含む国際法の完全かつ無条件な適用を口実として利用していることは、さらにいっそう遺憾である」。“Statement by the Permanent Mission of Russia to the UN on its non-participation in the UN Security Council Arria-Formula Meeting on Cyber Stability, Conflict Prevention and Capacity Building, Organized by Estonia on 22 May,” Permanent Mission of the Russian Federation to the United Nations, May 22, 2020, https://russiaun.ru/en/news/arria_220520.

[10] “Information Security Fact Sheet 2019”. 政府専門家会合の権限は、情報セキュリティ分野における現在および将来の脅威に対処するために可能な協力措置について検討し、検討結果を報告することである。United Nations General Assembly, *Resolution Adopted by the General Assembly on 22 December 2018, 73/266. Advancing Responsible State Behaviour in Cyberspace in the Context of international Security*, UN Document A/RES/73/266, January 2, 2019, p. 3 [hereinafter A/RES/73/266].

[11] A/RES/73/266, p. 3.

[12] United Nations Institute for Disarmament Research and Center for Strategic & International Studies, *Report of the International Security Cyber Issues Workshop Series*, 2016, p. 4 [hereinafter *UNIDIR & CSIS Report*].

[13] Ibid., p. 22; United Nations General Assembly, *Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 72nd Session, UN Document A/72/327, August 14, 2017, pp. 3-5; United Nations Office of Disarmament Affairs, “Group of Governmental Experts,” https://www.un.org/disarmament/group-of-governmental-experts/.

[14] *UNIDIR & CSIS Report,* pp. 5-6. 第１回（2004 年～2005 年）および第５回（2016 年～2017 年）ではコンセンサスが形成されず、手続上の報告書が提出された。
[15] Ibid., pp. 4-5.
[16] Ibid., p. 5.
[17] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 68th Session, UN Document A/68/98, June 24, 2013, para. 19.
[18] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 70th Session, UN Document A/70/174, para. 24.
[19] Ibid., para. 28 (d); Elaine Korzak, "International Law and the UN GGE Report on Information Security," Just Security, December 2, 2015, https://www.justsecurity.org/28062/international-law-gge-report-information-security/.
[20] Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," Just Security, June 30, 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-adavance-cyber-norms/.
[21] Schmitt and Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms"; キューバは「国際人道法は、情報通信における戦争および軍事行動のシナリオを合法化してしまうだろう」と述べている。Representaciones Diplomaticas de Cuba en el Exterior, "71 UNGA: Cuba at the Final Sessions of Group of Governmental Experts on Developmemts in the Field of Information and Telecommunications in the Context of International Security," June 23, 2017, http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information. 中国は、2019 年のオープンエンド作業部会においても「武力紛争法と武力行使法の適用可能性は、慎重に論じる必要がある。サイバー戦の合法性は、いかなる場合にも認めるべきではない」と述べている。"China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," p. 6, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.
[22] Nele Achten, "New U.N. Debate on Cybersecurity in the Context of International Security," Lawfare, September 30, 2019, https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security.
[23] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary armed Conflicts*, 33rd International Conference of the Red Cross and Red Crescent 9-12 December 2019, October 2019, p. 21 [hereinafter *ICRC IHL Challenges Report 2019*]; Mačák, "From Vanishing Point Back to the Core: the Impact of the Development of the Cyber Law of War on General International Law"; Schmitt and Vihul. "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms".
[24] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I. C.J. Reports 226, 1996*, para. 86.
[25] なお、武力紛争法が適用されない場合、サイバー行動を規律するのは、国際人権法となる。Schmitt and Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms".
[26] Ibid.; Anders Henriksen, "The End of the Road for the UN GGE process: the Future Regulation of Cyberspace," *Journal of Cybersecurity*, 2019, pp. 4-5.
[27] United Nations General Assembly, *Resolution adopted by the General Assembly on 5 December 2018 73/27. Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Document A/RES/73/27, December 11, 2018, p. 5, para. 5.
[28] Jürg Lauber, "Chair's Letter on Extending the Mandate of OEWG," June 5, 2020, https://front.un-arm.org/wp-content/uploads/2020/06/200605-oewg-chair-letter-on-extending-mandate.pdf; Jürg Lauber, "Chair's Letter with Draft Decision for the Postponement of the Third Substantive Session of the OEWG," June 9, 2020, https://front.un-arm.org/wp-content/uploads/2020/06/200609-oewg-chair-letter-with-draft-decision-for-postponement.pdf.
[29] Ibid.

[30] 報告書第 1 次仮草案に対するコメント（Comment by Member States on the initial pre-draft of the OEWG report）として国際人道法の適用可能性に対する各国の立場が示されている。“Open-ended Working Group,” United Nations, https://www.un.org/disarmament/open-ended-working-group/. ルクセンブルクおよびパキスタンが国際人道法の適用を認めたことの報告。“2nd Meeting of the First Substantive Session of the Open-Ended Working Group (OEWG) (Reports 9 Sep 2019),” the GIP Digital Watch Observatory, https://dig.watch/resources/2nd-meeting-first-substantive-session-open-ended-working-group-oewg. エジプトが国際人道法の適用を認めたことの報告。“Rules, Laws, and Norms: Stakeholders’ Commitments to Rules, Norms, and Principles (Reports 3 Dec 2019 16:00-19:00),” the GIP Digital Watch Observatory, https://dig.watch/sessions/rules-laws-and-norms-stakeholders-commitments-rules-norms-and-principles.

[31] “Second ‘Pre-Draft’ of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security,” Open-ended Working Group, May 27, 2020, p. 5, https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf.

[32] Ibid., p. 5, para. 29.

[33] Ibid.

[34] Ibid., p. 6, para. 32.

[35] 国際赤十字・赤新月運動規約第 5 条（赤十字国際委員会）第 2 項 G「武力紛争に適用可能な国際人道法の知識の理解及び普及に努め、その発展に寄与すること」。「国際人道法と ICRC」赤十字国際委員会、http://jp/icrc.org/humanity/.

[36] 赤十字・赤新月国際会議は、原則として 4 年ごとに開催される国際赤十字・赤新月運動の最高決議機関であり、赤十字国際委員会、国際赤十字・赤新月連盟、各国の赤十字社に加えて、ジュネーヴ諸条約締約国政府の代表が参加する。会議では、各種の人道的な課題や、ジュネーヴ諸条約その他の条約の制定に向けての提言などが行われる。「国際赤十字の成り立ち」日本赤十字社、http//www.jrc.or.jp/about/naritachi.

[37] *ICRC IHL Challenges Report 2019*, p. 2.

[38] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary armed Conflicts*, 31st International Conference of the Red Cross and Red Crescent 28 November - 1 December 2011, October 2011, pp. 36-38; *ICRC IHL Challenges Report 2015*, pp. 39-44; *ICRC IHL Challenges Report 2019*, pp. 18-22. 赤十字国際委員会の理解では、「サイバー戦」とは「コンピュータ、コンピュータ・システムまたはその他の接続されたデバイスに対するデータ・ストリームを通じたオペレーションであって、武力紛争の文脈において戦闘の手段または方法として使われる」もののことである。*ICRC IHL Challenges Report 2019*, p. 19.

[39] 赤十字国際委員会は、2018 年に、サイバー行動による潜在的な人間の損失について、専門家会合を開催、翌 2019 年 5 月、当該会合の報告書を公表している。*The Potential Human Cost of Cyber Operations, ICRC Expert Meeting 14-16 November 2018*, ICRC, May 2019. また、赤十字国際委員会は、2019 年 11 月に、国際人道法と武力紛争中のサイバー行動について、サイバー政府専門家会合およびオープンエンド作業部会に対して方針説明書を提出。ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflict*, ICRC Position Paper, November 2019, https://www.icrc/en/document/international-law-and-cyber-operations-during-armed-conflicts.

[40] *ICRC IHL Challenges Report 2019*, p. 18.

[41] Ibid., p. 19. これに対して、サイバー行動を避けることによって人間の損失が生じる可能性を指摘したものとして、Gary P. Corn, “The Potential Human Costs of Eschewing Cyber Operations,” Humanitarian Law & Policy, May 31, 2019, https://blogs.icrc.org/law-and-policy/2019/05/31/potential-human-costs-eschewing-cyber-operations/.

[42] *ICRC IHL Challenges Report 2019*, p. 19.

[43] Ibid.

[44] Ibid., p. 20.

[45] Ibid.
[46] API 第 1 条第 2 項「文民および戦闘員は、この議定書その他の国際取極がその対象としていない場合においても、確立された慣習、人道の諸原則および公共の良心に由来する国際法の諸原則に基づく保護並びにこのような国際法の諸原則の支配の下に置かれる」。
[47] ここでは、特別の保護対象の中でも特に、医療組織の保護と文民たる住民の生存に不可欠な物の保護が問題となっている。1949 年ジュネーヴ第 1 条約第 19 条；1949 年ジュネーヴ第 4 条約第 18 条；API 第 12 条および第 54 条。
[48] API 第 48 条。
[49] API 第 51 条第 5 項(b)。
[50] API 第 57 条第 2 項。
[51] API 第 58 条。
[52] API 第 51 条第 1 項および第 2 項。なお、赤十字国際委員会は、監視および虚偽の情報に対する法的評価には、武力紛争法だけでなく、国際人権法等、他の国際法が関係する可能性も指摘している。
[53] *ICRC IHL Challenges Report 2019*, pp. 20-21.
[54] *Tallinn Manual 2.0*, p. 437, paras. 6, 7 (Rule 100).
[55] Ibid., para. 6 (Rule 100). なお、少数派の見解は、*ICRC IHL Challenges Report 2015*（前掲注 2 参照）に同じ。
[56] Michael N. Schmitt, “The Notion of ‘Objects’ during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision,” Israel Law Review, Vol. 48, March 2015, p. 86.
[57] API 第 51 条第 1 項。
[58] API 第 49 条。
[59] *Tallinn Manual 2.0*, pp. 415-416, para. 3 (Rule 92).
[60] Ibid., p. 416, para. 4 (Rule 92). API 第 51 条第 5 項(b)および第 57 条第 2 項(b)。
[61] *Tallinn Manual 2.0*, p. 415 (Rule 92). なお、危害説では、対象の持つ機能にサイバー手段で介入（データの消去または改ざん）する場合について、次のようにさらに見解が分かれた。①機能回復のために当該対象の物理的な構成要素を換装することが必要となる場合には、損傷と認める（多数派）、②物理的な構成要素の換装に加えて、OS または特定のデータの再インストールが必要になる場合も、損傷と認める（多数派中の何人かの専門家）、③対象の持つ機能へのサイバー手段での介入は、損傷と認めない（少数派）。Ibid, pp. 417-418, para. 11 (Rule 92).
[62] Nils Melzer, *Cyberwarfare and International Law*, UNIDIR Resources, 2011, p. 26, https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf; Cordula Droege, “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protections of Civilians,” *International Review of the Red Cross*, Vol. 94 (886), Summer 2012, p. 558.
[63] Knut Dörmann, “Applicability of the Additional Protocols to Computer Network Attacks,” ICRC, 2004, p. 4, https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf; Melzer, *Cyber Warfare and International Law*, p. 26; Droege, “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protections of Civilians,” p. 559.
[64] API 第 52 条第 2 項；Dörmann, “Applicability of the Additional Protocols to Computer Network Attacks,” p. 4.
[65] Melzer, *Cyberwarfare and International Law*, p. 26; Droege,”Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protections of Civilians,” p. 559.
[66] API 第 52 条第 2 項。
[67] *Tallinn Manual 2.0*, p. 437, para. 6 (Rule 100).
[68] Heather A. Harrison Dinniss, “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives,” *Israel Law Review*, vol. 48 (1), 2015, pp. 39-54; Kubo Mačák, “Military Objectives 2.0: the Case for Interpreting Computer Data as Objects under International Humanitarian Law,” *Israel Law Review*, volume 48 (1), 2015, pp. 55-80; Melzer, *Cyberwarfare and International Law*, p. 31; Tim McCormack, “International Humanitarian Law and the Targeting

of Data," *International Law Studies*, volume 94, 2018, pp. 222-240.

[69] Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives," pp.42-44; Mačák, "Military Objectives 2.0: the Case for Interpreting Computer Data as Objects under International Humanitarian Law," pp.67-68.

[70] Michael N. Schmitt, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations," International Review of the Red Cross, Vol. 910, April 2019, p. 42.

[71] Michael N. Schmitt, "The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision," p. 86.

[72] データ非物体説の立場から対策を述べるものとして、Schmitt, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations," pp. 343-353. また、データ物体説の立場から、対策として新たな武力紛争法解釈を主張するものとして、Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives," pp. 50-54.

[73] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 68th Session, UN Document A/68/156/Add.1, September 9, 2013, p. 15 [hereinafter A/68/156/Add.1]; United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 71st Session, UN Document A/71/172, July 19, 2016, p. 12 [hereinafter A/71/172].

[74] オープンエンド作業部会において示された見解（脚注 33 を見よ。）のほか、オーストラリアについては、United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 66th Session, UN Document A/66/152, July 15, 2011, p. 6 [hereinafter A/66/152]; United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 69th Session, UN Document A/69/112, June 30, 2014, p. 2 [hereinafter A/69/112]; Australian Mission to the United Nations, "Annex A," *Australian Paper - Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, September 2019, pp. 5, 8 [hereinafter "Australian Paper Annex A"]. カナダについては、A/68/156/Add.1, p. 4. スイスについては、A/69/112, p. 17. 英国については、United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 65th Session, UN Document A/65/154, July 20, 2010, p. 15; "Annex 1A-International Law Aspects," Develop, Concept and Doctrine Center, Ministry of Defence, *Cyber Primer 2nd Edition*, July 2016, p. 13 [hereinafter *UK Cyber Primer*]; Attorney General's Office and the Rt Hon Jeremy Wright MP, "Cyber and International Law in the 21st Century," Gov. UK, May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-21st-century. 米国については、A/66/152, July 15, 2011, pp. 18-19; *US DoD Law of War Manual*, pp. 1013-1014. フランスについては、United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 74th Session, UN Document A/74/120, June 24 2019, p. 22; Ministère des Armées, *International Law Applied to Operations in Cyberspace*, October 2019, pp. 12-13. ドイツについては、United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 70th Session, UN Document A/70/172, July 22, 2015, p. 7 [hereinafter A/70/172]. オランダについては、Government of the Kingdom of the Netherland, "Appendix : International Law in Cyberspace," *Letter of 5 July 2019 from the Minister of Foreign Affairs to President of the House of Representatives on the International Legal Order in Cyberspace*, AVT19/BZ129031, September 26, 2019, p. 5, https://governmnwnt.ni/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace. ノルウェーについては、Norwegian Ministry of Defence, *Manual of the Law of Armed Conflict*, 2013 (English-Language Edition 2018), p. 209 [hereinafter *Norwegian LOAC Manual*]. スペインについては、A/70/172, p. 13; A/71/172, p. 20. また、G7（フランス、米国、英国、ドイツ、日本、イタリア、カナダ）としても、「サイバー空間を通じた武力攻撃に対し、国家が、国際人道法を含む国際法に従う」こ

とを確認している。*G7 Declaration on Responsible States Behavior in Cyberspace*, Lucca, April 11, 2017, https://www.mofa.go.jp/mofaj/files/000246367.pdf; G7 *Principles and Actions on Cyber*, p. 1, https://www.mofa.go.jp/mofaj/files/000160315.pdf.

[75] *US DoD Law of War Manual*, pp. 1020-1026; United States Department of Defense, *Cyberspace Operations*, Joint Publication3-12, June 8, 2018, p. IV-3; *UK Cyber Primer*, p. 14, n. 15; Ministère des Armées, *International Law Applied to Operations in Cyberspace*, pp. 12-16; *Norwegian LOAC Manual*, pp. 209-214. 米国防総省は、厳密には戦争法（武力紛争法）が適用されない場合であっても、軍事的必要性、比例性原則、区別原則のような戦争法の諸原則を軍事的なサイバー行動の計画および遂行の指針とするとの見解を示している。Hon. Paul C. Ney, Jr., "DoD General Counsel Remarks at U.S. Cyber Command Legal Conference," US Department of Defense, March 2, 2020, https://www.defense.gov/Newsroom/Speechs/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

[76] *Tallinn Manual 2.0*, p. 464 (Rule 100(b)). なお、タリン・マニュアル 2. 0 によれば、「サイバー兵器」とは、人の傷害若しくは死亡または物の損壊を発生させるために使用、設計またはその使用が意図されるサイバー手段を指し、「サイバー戦の手段」は、サイバー兵器およびサイバー兵器システムの双方を言い、サイバー攻撃のために使用、設計または使用が意図されるサイバー装置、資材、機器、機材、ソフトウェアを含む。他方、「サイバー戦の方法」とは、敵対行為を遂行するためのサイバー戦術、技術および手続を言い、攻撃に至らない広範なサイバー行動を含む。*Tallinn Manual 2.0*, pp. 452-453, paras. 1-5 (Rule 103). これに対し、ビラーおよびシュミットは、サイバー能力（サイバー攻撃で使用する装置およびソフトウェア）を戦闘手段とせず、サイバー行動と位置付けた上で戦闘方法に分類し、合法性審査を検討している。Jeffrey T. Biller and Michael N. Schmitt, "Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare," *International Law Studies*, Vol. 95, 2019, pp. 179-225.

[77] API 第 87 条第 2 項。

[79] API 第 57 条第 2 項。

[80] A/66/152, p. 19; United States Department of Defense, *Joint Targeting*, Joint Publication 3-60, January 31, 2013, p. A-1; "Australian Paper Annex A," p. 6; Paul Ducheine and Terry Gill, "From Cyber Operations to Effects: Some Targeting Issues," Ministerie van Defensie, *Militair Rechtelijk Tijdschrift, Jaargang 111 – 2018-3 Cyber Special*, p. 39.

[81] Paul Ducheine and Terry Gill, "From Cyber Operations to Effects: Some Targeting Issues," Ministerie van Defensie, *Militair Rechtelijk Tijdschrift, Jaargang 111 – 2018-3 Cyber Special*, p. 39.