NIDS 防衛研究所
The National Institute for Defense Studies

サイバー戦と国際法

理論研究部政治・法制研究室　　河野　桂子

NIDSコメンタリー　　第 40 号 2014 年 11 月 7 日

はじめに

本年 9 月に開催された NATO ウェールズ・サミットでは、初めて公式の場でサイバー攻撃が集団的自衛の対象となることが明言されたが、その直後から早速、懐疑的な見方が方々から提起されている。自衛権を発動するためのサイバー武力攻撃の定義が定まっていないのは勿論のこと、その他にも様々な課題が山積しているものと推測される。ただしサイバー攻撃に対する自衛権の論点は、既に別稿で論じたため、本稿ではそれ以外の問題について、主に国際法の観点から考察することとし、そのための素材として、以下のようなサイバー攻撃の想定事例を取り上げてみたい（拙稿「サイバー・セキュリティとタリン・マニュアル」防衛研究所ブリーフィングメモ（2013 年 10 月）参照）。

20XX 年、大規模サイバー攻撃を受けた A 国の国家元首は、「戦争行為」に対する自衛権の発動を表明し軍事作戦を開始した。このサイバー攻撃は、B 国に作戦拠点をおく非国家武装勢力 Z によるものと強く疑われているが、C 国、D 国、E 国など多数の国々のサイバー・インフラを踏み台にしていた。A 国は、すべての関係国に対して協力を求めたが、B 国、C 国および D 国は A 国を満足させる対応をとることはできなかった。こうした状況のもとで A 国は B、C、D の各国政府の許可を得ずに非国家武装勢力を掃討するための作戦、あるいはこの武装勢力によるサイバー攻撃を中断するための措置を各国領域内で講じた。

A 国に対するサイバー攻撃の作戦拠点が置かれた B 国も、遠隔操作により領域内の端末が攻撃の踏み台に悪用された C 国、D 国、E 国のいずれも、A 国との間で敵対関係にはなく、直接の武力紛争当事者（交戦国）ではない。しかし、B 国、C 国、D 国からの同意を得ずに A 国が軍事作戦を遂行することは国際法上、果たして許容されるのだろうか。

1　サイバー戦に適用される国際法とは

この政府による「戦争行為」の認定は、多分に政治的な意味合いが強いが、サイバー攻撃が国際法上の開戦行為に該当するには、その性質と烈度の条件をともに満たすことが必要である。軍事的反撃に訴える法的根拠を定めるのが自衛権だが、それとは別に戦闘の手段と方法を規制するのが武力紛争法（国際人道法）である。特にサイバー戦に着目した武力紛争法のルールは、2012 年に NATO サイバー防衛センターが 2012 年に公表した「サイバー戦に適用される国際法タリン・マニュアル」に詳しく記されている。

平時であると戦時であるとを問わず、データの窃取やホームページの改ざんなどのサイバー攻撃が行われた数は枚挙にいとまがないが、法的な意味における戦闘行為が実際に行われた例があるのか否かは、公式に報道された例はまだなく真偽は不明である。いずれにしても、ある軍事行動が開戦行為に該当するには、散発的でなく結果が重大であるなどの烈度要件を満たす必要があると言われることが多く、ミサイルや爆弾などの在来の兵器と組み合わせずにサイバー手段だけで戦を開くのは法的には敷居が高い（ただし、国家間戦争については烈度要件を不要とみる立場もあり論争がある）。

このこととは対照的に、ミサイルや爆弾の使用によって始まった武力紛争の最中にサイバー手段が使われた場合、法的な意味で戦闘行為に該当するサ

イバー攻撃は数多くありうるものと考えられる。武力紛争中の個別の戦闘行為には烈度要件が課されないためであり、軍のレーダーや指揮通信システムを無力化するなど敵の軍事作戦に悪影響を与えるもの、あるいは民用物に「損害」を与えるようなサイバー攻撃などがそれにあたる。この「損害」の範囲については解釈がまだ確定していないが、少なくとも軍に対するサイバー攻撃が法的な戦闘行為と認定されるために物理的損害の発生を待つ必要がないことは、電子戦の中でも電波妨害（ジャミング）が従来、法的な戦闘行為とみなされてきたことからも明らかである（2009 年にハーバード大学人道政策紛争研究プログラム（HPCR）が刊行した「空・ミサイル戦に関する国際法マニュアル」のルール 1(m)を参照）。このように武力紛争中のサイバー攻撃の法的規制は、サイバー単独の武力攻撃に対する自衛権が未知の問題であるのと比べて、はるかに現実味があり、かつ実務上早期の整理を要する問題である。サイバー戦に適用される国際法に関しては、現在も国連第 1 委員会サイバー・セキュリティ政府専門家グループ（GGE）でも議論が続けられているが、自衛権の保護法益をめぐり西側諸国と対立するロシアでさえも、サイバー戦に武力紛争法が適用されることについては肯定的見解を示しており、細部の解釈適用問題を議論するための土台は固まりつつあると言える。

2 サイバー攻撃の中継地国の責任

既に広く知られている通り、米国は、アルカイダに対する自衛措置の一環として、アフガニスタン以外の国でも軍事作戦を遂行し、2011 年 9 月 30 日には「アラビア半島のアルカイダ」（AQAP）の幹部であり米国籍を有するアンワル・アル・アウラキ（Anwal Al-Aulaki）がイエメン国内を車両で移動しているところを無人機による標的攻撃作戦で殺害した。この作戦をめぐっては、アウラキ氏の父親などが米国政府高官に対して憲法違反の訴えを提起していたが、本年 4 月 4 日、コロンビア特別区連邦地方裁判所は、被告側の訴え却下の申立てを受入れて原告の訴えを斥け、この判決はその後確定している。米国政府は、非国家武装勢力との武力紛争を戦うに際して、地理的な境界を領域国の同意または管理責任に応じて柔軟に捉えているようである（イエメンは前者に該当する）。サイバー攻撃の文脈では、まだこのような実例は存在しないが、米国防省が数年前に公表した文書を見ても、同様の措置がとられる可能性は高いように思われる。

非国家主体との武力紛争については、最低限の人道的原則として 1949 年の戦争犠牲者の保護に関するジュネーヴ諸条約共通第 3 条が用意されており、政府軍が非国家武装勢力のメンバーの身柄を捕らえたときの拷問などの非人道的待遇を禁止しているが、非国家主体との間の戦闘を規制する国際法は勿論この条文だけではない。1977 年のジュネーヴ諸条約第 2 追加議定書は、政府軍と戦う反政府武装勢力が一定領域を実効支配していることなど適用条件が厳格であり、国境をまたいだ非国際的武力紛争にそのまま適用されるとは考えがたいが、国際慣習法化した同議定書の諸規則が適用されることは異論の余地がない。

これ以外にも、伝統的な中立法からの類推により、非国家武装勢力の拠点がある領域国に一種の管理責任が求められるという考え方が一部の国家実行や学説で提唱され始めている。2011 年 11 月付で起案された米国司法省の「アルカイダまたは関連勢力の作戦幹部である米国民に対する殺害作戦の合法性」と題する文書では、領域国が、その領域内に拠点をおくアルカイダなどの脅威を除去する能力を持たないか、またはその意思がない場合に米国自ら作戦を実施することは中立法に合致すると述べられている。仮に中立法が妥当しないとしても、両武力紛争当事者に対して公平な立場を求める中立法ですら領域国に対して管理責任を求めるのであれば、同盟国または友好国との関係ではことさら、武装勢力を利さないための管理責任の履行が強く求められると考えられる。

1907 年にハーグ平和会議で採択された陸戦中立条約は、交戦国に対して、軍隊、弾薬、軍需品が中立領内を通過すること（第 2 条）や軍事利用目的の通信機器を中立領域内に設置すること（第 3 条）を

禁止しており、敵対目的によるサイバー・インフラの設置や利用も同様に禁止されると考えられる。他方、本条約は、私人による兵器弾薬の輸出（第 7 条）や、その所属が中立国か私人かを問わず電信、電話ケーブル、無線電信機を交戦国に利用させること（第 8 条）は禁止していないが、その理由は、これらの活動が平時でも許される種類の活動とみなされてきたためであり、物品が後で他方交戦国によって没収されても、元の所有者である中立国私人やその本国の政府は抗議を行うことはできない。

陸戦中立条約第 8 条をサイバーの文脈に照らして解釈すると、非国家武装勢力がサイバー攻撃の中継地としてインターネットを利用することは条約上の禁止に該当せず、領域国がそれを放置しても何ら国際的な責任は発生しないと考えられる（先述の「HPCR 空・ミサイル戦に関する国際法マニュアル」ルール 167(b)はこうした見方を採用している）。他方、そうしたデータ通信にマルウェアが添付されており、それを用いたサイバー攻撃が戦闘の一環として行われる場合には単なる通信の域を超えていることから、A 国はそれを到底、看過しえないものと考えるだろう。「タリン・マニュアル」は、中立国に対してどの程度の管理責任を負わせるかについて意見の一致を見なかったが、少なくとも中立領内端末が乗っ取られ、有害なファイルの中継地として利用された場合には、陸戦中立条約第 2 条が禁止する武器弾薬の輸送に該当すると考えた専門家が多数いたようである。この考え方に従えば、重大かつ深刻なサイバー攻撃の中継国が、被害国から捜査や取締を要請された後もそれを怠るか、または取締を試みるも不首尾に終わるという例外的な状況のもとでは、中継国が同意を与えない場合であっても A 国が自ら掃討作戦を実施することが許されるという帰結が得られよう。ただし、サイバー攻撃が容易に国境を越えて展開されることに鑑みると、非国家武装勢力によるサイバー攻撃をきっかけとして、武力紛争地域もまた同じく容易に、また無限大に拡大する懸念が持たれる。

そもそも各国間のサイバー能力や、IT 依存度とそれに由来する脆弱性については大きな開きがある。さらにサイバー攻撃は、コードを書き変えるだけで無限大に攻撃を続けることが可能であり、数が有限である在来の兵器とは性質が全く異なる。上記の C 国のサイバー能力が低い場合には、数多くの攻撃拠点が遠隔操作により構築され、A 国に取締要請を受けても自力で対処できず、十分に期待に応えることはできないかもしれない。無人機による殺害作戦の場が主に破綻国家や内戦中の国家であったのと比べて、サイバーの文脈では、たとえ先進国であっても自国の意にそぐわない作戦が自国領域内で行われないとは限らないと危惧される。

3 IT 技術者は軍事目標か？

サイバー戦に限らず、非国家主体と戦う戦闘に適用される国際法については、まだ解釈が未確定な部分もある。例えば、非国家武装勢力の思想に共鳴した D 国の IT 技術者がマルウェアの研究開発に協力したとする。ひっきりなしにサイバー攻撃に受け続ける A 国が D 国の制止も聞かず、自衛権を根拠にこの技術者を殺害した場合、この殺害行為は合法と言えるだろうか。これは、いわゆる「文民の敵対行為への直接参加」（1977 年ジュネーヴ諸条約第 1 追加議定書第 51 条 3、および同第 2 追加議定書 13 条 3）の問題である。両追加議定書は、文民は、敵対行為に直接参加していない限り、攻撃の対象とされてはならないと定める。仮にこの技術者の武装勢力に対する協力が一般的な IT 技術の指導か、あるいは A 国に対して使用する DDoS 攻撃用のマルウェア開発にとどまる場合には、「戦闘行為への直接参加」とみなされる可能性は低い。他方、この技術者が A 国の軍事通信システムの機能障害をもたらすマルウェアを開発し、かつ作戦を遂行した場合には、「戦闘行為への直接参加」に該当することは疑いの余地がないだろう。ただし、この後者の場合であっても、いったんこの技術者が戦列を離れ、帰国の途に就いたならば、「戦闘行為への直接参加」は

終了したものとみなされ、D 国の自宅居間でくつろぐこの技術者を A 国が殺傷するのは違法である。

国家の正規軍と異なり、非国家武装勢力については組織に属する全てのメンバーが常に合法的な軍事目標に該当するのか否かをめぐり議論が収束していない。単に一員であるという理由だけで後方業務につく者まで広く軍事目標に含めるという考え方は、従来、正規軍の構成員については通用している。しかし、非国家武装勢力にもこの考え方をそのまま当てはめれば、上記の IT 技術者のように組織には正式に属さずに一定期間に限り戦闘に加わる協力者までもが同様に殺傷されるリスクがあり、戦争犠牲者の保護を趣旨目的とする国際人道法に反するという批判が提起されている。ここで主に懸念されているリスクとは、Z のメンバーと行動を共にしていることにより巻き添えの損害を受けることではなく、むしろ、IT 技術者が直接の攻撃対象とされるリスクのことである。A 国は、この IT 技術者の能力が武装勢力によるサイバー攻撃の不可欠の要素とみなして、より優先度の高い軍事目標とさえ考えるかもしれない。確かにこの IT 技術者は、軍事施設に対するサイバー攻撃に従事している間は、正当な軍事目標に該当するが、それが終われば本来、A 国による攻撃から保護されるべき地位を回復する。ただし、非国家武装勢力は、正規軍と異なり、帰属の形式的条件が不明瞭であることが多く組織外の協力者との区別も容易ではないため、A 国から見れば「一員」に対する攻撃も、一員ではない単なる一時的協力者の多くを A 国の攻撃にさらす危険があるという懸念である。この見解に対しては反論も多く、国家の正規軍がその時点の任務の種類とは無関係に常時攻撃対象であるのと比べて武装勢力を優遇する結果を生み不当であるとか、武装勢力に対する協力者は自らも攻撃にさらされるリスクを受け容れるべきだという主張が提示されている。

なお、この IT 技術者が帰国前に、非国家武装勢力 Z の一員であり、Z 内で語学や思想の教育指導にもっぱら携わるメンバーと行動を共にしていたところ、A 国部隊の突撃を受け負傷したとする。A 国は、合法的な攻撃の結果生じた付随的損害であり、受忍限度の範囲内であると説明したが、上述の後者の考え方に従えば、この A 国の主張は妥当である。しかし、前者の考え方に従えば、この語学や思想教育に従事する Z の一員は、そもそもこの時点では合法的な軍事目標に該当しないため、その近傍にいたために IT 技術者が被った巻き添えの被害は、均衡を失するどころか違法な攻撃の結果によるものであり、法的に正当化されない。

「タリン・マニュアル」のルール 35 はこの問題を取り上げているが、専門家の間では意見が割れたために、前述の 1977 年第 1 追加議定書第 51 条 3、および同第 2 追加議定書第 13 条 3 に定めた文言以上の内容を盛り込むことはできなかったようである。ルール 35 の注釈には、正規軍と非国家武装勢力の構成員を同一視する監修者の考え方が色濃く反映されているが、細部はまだ現行法としてまだ確立していない以上、参照時には注意が必要である。

おわりに

領域国の責任や非国家武装勢力に関与する個人の地位は、いずれも新しい問題ではないがサイバー攻撃との関連でも重大な結果を招く恐れがあることを本稿では整理した。サイバー戦に適用される現行国際法を記述した「タリン・マニュアル」においても、これらの点を含む多くの解釈適用上の問題点が浮き彫りにされており、国連におけるサイバー・セキュリティをめぐる議論でもそれらの論点を一つ一つ点検することが望まれる。

（10 月 24 日脱稿）

プロフィール profile

理論研究部
政治・法制研究室
河野　桂子

専門分野：国際法（武力紛争法）

防衛研究所企画部企画調整課
直　通：03-3713-5912
代　表：03-5721-7005（内線 6584, 6522）
ＦＡＸ　：03-3713-6149
※ 防衛研究所ウェブサイト：http://www.nids.go.jp