ブリーフィング・メモ

サイバー・セキュリティとタリン・マニュアル

理論研究部　政治・法制研究室　主任研究官　河野　桂子

はじめに

サイバー攻撃を受けた被害国は、国際法上、軍事力を用いて反撃することが許されるのか。それとも従来のサイバー犯罪への対応と同様、警察機関の法執行に依らなければならないのか。2007 年の対エストニア・サイバー攻撃を受け、NATO のサイバー防衛能力の強化を目的として設立された NATO サイバー防衛センター（NATO CCD COE）は、昨年、3 年がかりの研究成果「サイバー戦に適用される国際法に関するタリン・マニュアル」（以下、タリン・マニュアル）を発表し、サイバー攻撃に対しては一定の条件のもとで軍事的対応をとりうるとの見解を示した。

国連憲章第 51 条は、「この憲章のいかなる規定も、国際連合加盟国に対して武力攻撃が発生した場合には、安全保障理事会が国際の平和及び安全の維持に必要な措置をとるまでの間、個別的又は集団的自衛の固有の権利を害するものではない。」と定め、武力攻撃の被害国に対して反撃の権利を認めている。しかし、いかなる場合に「武力攻撃」が発生すると言えるのかについては諸国の実行ないし学説でも未だに一致した見解はない。タリン・マニュアルが主たる検討対象としたのは、サイバー戦に適用可能な現行国際法（lex lata）であるが、自衛権の解釈をめぐる現況に鑑みると、その試みは野心的であるとさえ言える。本稿では、特に本文書の大きな特徴と思われる以下の３つの論点を取り上げ、そこで提示されたタリン・マニュアルの立場が果たして現行法原則としての性格を備えているかを探ることとしたい。第１に、サイバー武力攻撃に対する先制的自衛は許されるのか否か、第２にどのようなサイバー・オペレーションが武力行使に該当するのか、第３に、対テロ戦争の例でも明らかなように、パキスタンやイエメンなど様々な国におかれたテロ組織のサイバー・オペレーションの拠点を、領域国の同意を取り付けずに攻撃することが許されるのか否かである。これらの３つの論点は、いずれも国際法上いつ武力を使うことができるのか、という武力行使の正当性を規律する法（jus ad bellum）に分類される。タリン・マニュアルでは、上記の jus ad bellum に関する議論に加えて、武力紛争法（jus in bello。戦争法や国際人道法とも称される）も扱っているが、本稿では紙幅の制約から前者の論点を中心に取り上げる。

なお、タリン・マニュアルは、法律家や実務家が個人の資格で参加した国際専門家会合によって起草された学術研究成果であり、国際合意でも NATO 防衛センターの公式見解でもない。したがって、本文書自体には形式的意味での法源としての価値はない。ただし、同じく非公式文書として過去に作成された「海上武力紛争に適用される国際法に関するサンレモ・マニュアル」が、英国国防省刊行の『武力紛争法マニュアル』に大幅に採り入れられている例もあり、実質的な意味において現行国際法を反映している場合には、タリン・マニュアルが今後の国家実行に採用される可能性も無視できない。

自衛権の行使要件

まず、本論に入る前に jus ad bellum の枠組みを確認しよう。第１に、国連憲章第 2 条 4 項は、他国

に対する武力の威嚇又は武力の行使を禁止するが、被害国が自衛権によって反撃を許されるのは、「武力攻撃に該当する最も重大な形態の武力行使」に対してだけである。つまり、武力行使と武力攻撃との間にはギャップがあり、武力攻撃に至らない、より重大性の劣る武力行使に対しては、国連安全保障理事会が国連憲章第７章の強制措置によって対応するのが基本であり、被害国が軍事的対抗措置をとることは通説では許されていない。米国のように両者をほぼ同一視して、あらゆる武力行使に対して自衛権を発動する立場は少数説に属する。また第２に、武力攻撃が発生した場合でも、被害国は無制限に軍事力を使ってよいわけではなく、国際慣習法上、必要性や均衡性の要件に従わなければならない。以上の２つの点はいずれもタリン・マニュアルで採用されている。

（１）サイバー武力攻撃に対する先制的自衛

国連憲章第 51 条は「武力攻撃が発生した場合」に自衛権の発動を認めているが、その発生前でも武力攻撃が差し迫っている場合には自衛行動をとることが許されているとするのが先制論である。タリン・マニュアル注釈によれば、先制的自衛は国連憲章作成前から国際慣習法として確立した現行法であり、その効力は今でも失われていないという。ただし、従来の先制的自衛論の中には、武力攻撃の結果が発生する前でも武力攻撃自体が開始されたことで「武力攻撃が差し迫っている」とみなす主張もあった。こうした先制論は「武力攻撃」の範囲をめぐる解釈にも近似し、その限りでは先制論の妥当性を形式的に議論する意義は乏しかったが（ちなみに、我が国は我が国に対する急迫不正の侵害があることを自衛権発動の一要件とする）、タリン・マニュアルが採用する先制論は、これと異なり被害国が有効な防御措置をとる最後の機会か否かによって急迫性の条件を判断するものであり、場合によっては武力攻撃着手以前でも先制行動を許す考え方である。こうした先制論は、既に大量破壊兵器について提起されてきたが、攻撃の着手から被害発生までの一連の過程が瞬時で完成するサイバー攻撃の特性に照らして特に要請されるという。

なお、何がサイバー武力攻撃に該当するかについては、従来、航空管制システムや原子力関連施設へのサイバー攻撃などがよく例として引用されてきた。そうしたサイバー攻撃は、航空機の衝突や放射能の拡散など通常兵器の攻撃に匹敵する甚大な被害をもたらすというのがその理由である。タリン・マニュアルは一般原則として、「武力攻撃」の該当性を計る基準として「規模と効果」によることを提示したが、国際専門家会合は人命の損失や物の損壊などの物理的被害を伴わない広範な悪影響にとどまるサイバー・オペレーションが武力攻撃に該当するか否かについては合意に至ることができなかった。この問題は第２の論点にも関係するので、後にまた触れることとする。

ちなみに、タリン・マニュアルはサイバー空間のみで行われる戦闘（cyber-to-cyber operation, stricto sensu）を検討対象とするので、通常兵器攻撃との組み合わせでサイバー・オペレーションが行われる状況（例えば、2007 年 9 月にイスラエルがシリア空爆前に行った防空レーダーの操作など）については何も言及していない。けれども、おそらくタリン・マニュアルの考え方をもとにすると、先行するサイバー・オペレーション自体に物理的効果が伴わなくとも、後続する通常兵器攻撃と一体のものとみなされることによって、武力攻撃の発生又は急迫性が認定されるものと思われる。

（２）サイバー武力行使の範囲

武力行使は、前述のようにそれ自体は自衛権を発動させないが、武力行使がなければ武力攻撃も存在しえない点で、タリン・マニュアルでも極めて重要な論点として位置づけられている。

何がサイバー空間の武力行使に該当するかについてタリン・マニュアルは、武力攻撃の問題と同様に具体的基準はないとし、従来兵器の武力行使に相当する「規模と効果」を判断基準とした。続く注釈によれば、現行法上、人の死傷や物の損壊など物理的被害をもたらすサイバー・オペレーションだけが武力行使に該当するという。その一方で、物理的被害を伴わないサイバー・オペレーションであっても、将来、諸国の実行等によって武力行使と認定される可能性があるという。注釈では、その判断の目安となりうる８つの要因（①結果の重大・深刻性、②即時性、③直接性、④侵入性、⑤結果の計測可能性、⑥軍事的性質の有無、⑦国家の関与の程度、⑧合法性の推定など。ただし例示列挙であり他の要因もありうる）が列挙されているが、監修者を含む一部のメンバーによれば、そうした傾向は既に国家間で芽生えているという。例えば、オランダの国際問題政府諮問評議会及び国際公法問題諮問委員会の共同報告書（2011 年）によれば、国家機能の深刻かつ長期的な崩壊をもたらす組織的サイバー攻撃や、軍の動員を不可能にするほど大規模な軍事通信ネットワーク全体に対する攻撃は、武力攻撃に該当しうるという。

上記の議論は、サイバー対サイバーの戦闘であれば実際的問題を惹起することはないが、いずれの国も従来兵器による軍事的対抗措置の選択肢を捨てていないため、どのようなサイバー・オペレーションが武力行使さらには武力攻撃に該当するのかについて事前に共通の理解を持つことが、過大評価に基づく戦争勃発又は拡大の危険を避けるためにも望ましい。タリン・マニュアルが今後の議論の素材となり国家実行を触発することが期待される。

（３）サイバー攻撃拠点がある第三国への自衛権発動

近年、パキスタンやイエメンなどで行われている無人機による殺害攻撃に対して激しい批判が繰り広げられているが、米国政府の説明によれば、それらの軍事作戦は全て自衛に基づく措置であり、領域国が自ら取り締まる意思と能力を欠く場合には、被害国は直接行動をとる権利があるという。タリン・マニュアル国際専門家会合もこの考え方を支持し、非国家武装勢力やテロ組織が第三国を拠点としてサイバー攻撃を行う場合に、当該拠点に対する自衛行動を肯定している。つまり、サイバー空間の単なるデータの通過だけでは通過国の責任は発生しないものの、自国領域及び排他的管理を及ぼす場所（国外の軍事基地、公海とその上空、又は在外公館）のサイバー空間が、他国に悪影響を及ぼす行為の実施のために使用されることを把握しながら放置し適当な措置を講じない場合、被害国は自衛権に訴えることができるという。

仮にイエメンで既に内戦が発生しており、イエメン政府の派遣要請を受けてアメリカ軍が軍事作戦を展開している場合には、イエメン国内に拠点をおくテロ組織がサイバー攻撃に従事していようと、アメリカ軍が無人機を投入しようと、特に法的な問題はないかもしれない。しかし、内戦もまだ発生しておらず領域国政府が同意を与えていない場合には軍事的措置ではなく法執行によって対応すべきであると主張する論者も多い。タリン・マニュアルも上述の点について特段の国際判例や国家実行を引用しておらず、したがって現行法と断定するには時期尚早の感も否めない。

ただし批判論の中にも注意を要する内容が含まれている。一部の批判論者によれば、非国家武装勢力によるテロ攻撃は、領域国に帰属しない限り常に犯罪であり、したがって非国家武装勢力が同時多発テロに匹敵する被害をもたらすサイバー攻撃を行ったとしても、被害国は自衛権を発動できないとされる。非国家武装勢力が単独で武力攻撃主体となるかの問題は特に同時多発テロ以降、脚光を浴びているが、肯定的に解する国際的な傾向もあり慎重な議論が必要であると思われる。

おわりに

本稿では、特に jus ad bellum の観点からサイバー戦に適用される「現行法」が何かという問題をタリン・マニュアルを素材に検討し、中でも先制的自衛、武力行使の範囲、領域国が意思と能力を欠く場合の自衛権行使の可否の３つの論点を中心に取り上げたが、いずれも最近の国際的傾向を大いに取り込んだ要素が含まれているものの直ちに現行法と断定することはできない。ただし、タリン・マニュアルの立場を支持するか否かは別として、サイバー空間において鋭く現れる国際法上の論点が網羅的に扱われている点において、タリン・マニュアルが、今後、サイバーに関する国際合意が確立する過程において非常に大きな影響を与えることに異論の余地はない。サイバー空間の特質に鑑み先制的自衛は許されるのか、非国家武装勢力やテロ組織によるサイバー・テロは国際法上、どのように評価され、いかなる場合に軍事的対応が許され、あるいは許されないのか、いずれの論点も早期の解決を要する課題である。

（平成２５年１０月８日脱稿）

参考文献

・Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence /General Editor Michael N. Schmitt (Cambridge University Press, 2013) <http://www.ccdcoe.org/249.html>.

防衛研究所企画部企画調整課
外　線：０３－３７１３－５９１２　　専用線：８－６７－６５２２、６５８８
ＦＡＸ：０３－３７１３－６１４９　　※防衛研究所ウェブサイト：http://www.nids.go.jp