ブリーフィング・メモ

武力攻撃未満のサイバー攻撃に関する国際法―『タリン・マニュアル２』を題材に

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

2017 年２月、『サイバー活動に適用される国際法タリン・マニュアル２』（以下、『タリン２』）が刊行された。本書は、『サイバー戦に適用される国際法タリン・マニュアル』（以下、『タリン』）の続編であり、『タリン』と同様に、北大西洋条約機構サイバー防衛センター（NATO CCD COE）が主催した研究プロジェクトの一環として刊行された。実際に執筆したのは、同センターによって招集された実務家および国際法研究者である。特に『タリン２』には一部のアジア諸国（日本を含む）の専門家も参加した。

『タリン』および『タリン２』は、いずれも政府間の合意文書ではなく、文書の形式上は単なる学説である。それにもかかわらず、『タリン』はあたかも西側諸国の公式見解であるかのように、中国やロシアの政府関係者などによって批判されることがあり、おそらく『タリン２』も同様の事態に直面することが予想される。NATO がこれら両文書を専門家らに作らせた真の目論見は不明だが、対外的にはやはりその記述内容が西側諸国の政府の間で一定程度共有されたものとして受け取られている可能性が高い。また、そのような疑念が一部の国々に生ずる背景には、この問題をめぐる最近の状況が関係しているように思われる。

１．サイバー活動の国際的規制の現状

今日、サイバー活動に関する真に多数国間の国際条約は存在しない。2001 年サイバー犯罪条約は確かに違法なアクセスなど一部のサイバー犯罪の捜査および訴追について締約国間の協力を定めているが、締約国の数（56 カ国）も規律事項も限定的である。それ以外のサイバー活動の国際的規制を議論する場は今までのところ複数設けられており、代表的なものとして次のものを挙げることができる。①国際の平和および安全の文脈では国連総会第１委員会の下に設置されたいわゆるサイバー政府専門家会合（GGE）、②国際電気通信法の文脈では国際電気通信連合（ITU）、③人権（特にプライバシー権）の文脈では国連人権理事会、④G7 サミット（主要国会議）のとりわけ 2016 年伊勢志摩サミットに加えて、NATO も勿論のこと首脳会合などの場でこの問題に取り組んでいる。このうち、G7 やNATO のように西側諸国のみで構成される場を別として、サイバーGGE やITU のように中国、ロシアおよび両国に同調する国々が参加する枠組みでは、往々にしてこの問題に関する国際法規範の在り方をめぐって参加国間で意見が折り合わず、全参加国が賛同できるような合意を形成するに至っていない。このように政府間の交渉が遅々として進

展しない状況を背景として、『タリン２』は『タリン』と同様に、サイバー活動に関する現行国際法（lex lata）を明文化することを目標として掲げ、その際にサイバー以外の分野で発展をとげた国際法の諸規則に依拠した。

２．『タリン２』の概要

『タリン２』が主要な考察対象としたのは、平時のサイバー活動に適用される国際法である。ここで言う平時とは、武力攻撃に至らないサイバー攻撃が発生している状況である（武力攻撃に対しては自衛権の援用が認められているが、前作『タリン』に属する論点のため、本稿では割愛する）。以下では、被害国のとりうる対応と諜報活動の法的根拠について『タリン２』の専門家らがどのような整理を行ったのかを概観する。

（１）武力攻撃未満のサイバー攻撃に対する被害国の対応

武力攻撃未満のサイバー攻撃とは、言い換えれば、主に武力の行使および威嚇（規則68）、違法な干渉（規則 66）および主権侵害（規則 4）に相当するサイバー攻撃のことである。サイバー武力行使の典型例として『タリン２』の専門家らが念頭においたのは、2010 年に発覚したスタックスネット攻撃（ウラン濃縮用の遠心分離機の破壊）である。サイバー攻撃による主権侵害とは、本質的な政府の機能（社会保障、選挙、徴税、外交、国防など）に不可欠なデータが改変または破壊され業務が妨害された場合を指す。2015 年に発覚した日本年金機構へのサイバー攻撃がこの例に該当する。違法な干渉とは、国内および国際問題の意思決定について、サイバー攻撃によって強制的に変更させることを指す。

『タリン２』によれば、被害国は、加害国が自国に対して負う法的義務を遵守させるために、この加害国に対して対抗措置をとることができる（規則 21）。つまり被害国は、加害国の主権を侵害するようなサイバー攻撃を行うことが認められ、しかもその違法性は阻却される。ただし、この対抗措置は武力を用いたものではあってはならない。

サイバー武力行使は『タリン』によれば、人の死亡もしくは傷害または物の物理的損壊の発生が要件とされている。また、軍用機が他国の領空に侵犯した場合と、サイバー作戦要員が他国領域内の情報ネットワークにハッキング（電子的仮想的に侵入）した場合を比較すると、前者は通説の下では違法な武力行使とされるのに対して、後者は武力行使とはみなされない。物理的な侵入とは異なり、サイバー手段によってハッキングをしただけでは、その国の領土保全を侵害したとまでは言えないためである。勿論、サイバー犯罪条約の締約国間であれば、条約の定める違法なアクセス罪に該当するが、ロシア、中国または北朝鮮のいずれも同条約の非締約国である。あるいは非締約国であっても国内法上の犯罪（日本の例では「不正アクセス」）とみなすことは可能だが、不正アクセスと主権侵害は必ずしも同義とはされていない。

次に、前述の例（本質的な政府の機能の侵害）以外のいかなる場合にサイバー攻撃が被害国の主権を侵害すると言えるのかについて、『タリン 2』は明確な基準を見出すことができなかった。専門家らの間で合意されたのは、サイバー・インフラの部品交換を要する被害は、物理的な損害を与えたに等しく、それ故、物理的損害が生じた場合と同様に主権侵害にあたるという点だけである。しかし、部品の交換は特段要さず、分散型サービス妨害（DDoS）攻撃のように一時的にインフラの機能が失われる程度の被害しか生じない場合にまで、その国の主権を侵害するとは『タリン』の専門家は考えなかった。従って、対象国の本質的な政府の機能を侵害せず、その他の国際合意にも違反しないサイバー攻撃については、一時的な停電など復旧が容易なインフラの機能を喪失させても、それ自体は国際法上、合法行為とみなされる。物理的空間の文脈では、従来、非友好的であるが違法ではない報復（retorsion）という類型が存在することが指摘されており、その例として外国軍用機の領空侵犯に対する下空国のインターセプトまたは外国の軍艦による領海内有害航行に対する沿岸国海上当局の退去要請措置、または通航権を確認するための航行作戦などが学説上挙げられてきたが、サイバー手段についても同様に、それ自体合法な被害国の対応として一定のサイバー措置がありうることを『タリン 2』は示唆している。

（2）北朝鮮をめぐる一連のサイバー攻撃の評価

一部の報道によると、米国では、北朝鮮に対するサイバー攻撃を許可する（非公開の）大統領令が署名され、2017 年 9 月末までサイバー軍によって DDoS 攻撃が実施されていたと言われている。仮にこの報道が事実であるとして、ではこの北朝鮮に対するサイバー攻撃は北朝鮮による一連の核・ミサイル開発またはサイバー攻撃（例えば米韓両軍による対北朝鮮作戦計画の流出は北朝鮮によるものと疑われている。この論点について下記（3）を参照）に対する対抗措置として行われているのであろうか。北朝鮮による核ミサイル開発計画に対しては、既に国連安全保障理事会が国際の平和および安全に対する脅威と認定して経済制裁を実施しているが、サイバー関連の措置は制裁措置には含まれていない。また、米国が一連の安保理決議の違反を理由に、単独で対抗措置をとることは必ずしも認められていない。『タリン 2』も、そのような名目による対抗措置の許容性については消極的である（規則 24 解説 4 および 5）。

それでは、米国サイバー軍による対北朝鮮サイバー攻撃は、米国自身が北朝鮮から直接受けた被害（サイバー攻撃に限らない）を原因とする対抗措置として説明できるだろうか。あるいはそもそも合法的な報復に分類できるだろうか。2014 年にソニー・ピクチャーズ・エンターテイメント（SPE）に対するサイバー攻撃が発生して間もなく、北朝鮮のインターネットが一時的に遮断されたという報道が出回り、それが米国による措置であったとの噂が流れたことがあった。仮にそれが事実であったとしても、その措置は『タリン 2』が示した基準に基づき判断する限り、それ自体は合法的な対応である。最近行われたと言われている米国のサイバー軍による対北朝鮮 DDoS 攻撃についても、物理的被害の出ない一時的に不便な状況に被害がとどまるのであれば同様に合法である。他方、報道の真偽

は不明だが、北朝鮮のミサイル発射をサイバー攻撃によって阻止した作戦については、さきの主権侵害認定基準に照らして明らかに本質的な政府の業務を阻害しているので報復として説明することは難しい。北朝鮮による先行違法行為が何であったかは別として理論上その主要な正当化根拠は、対抗措置をおいて他に見当たらない。

（3）サイバー諜報の合法性

前述の（1）で考察した主権侵害の認定基準は、サイバー諜報の合法性にも大いに関係する。サイバー諜報が国際法上、合法か否かは、次の2点によって判断される。第1に諜報それ自体の合法性、第2に諜報の方法の合法性である。第1の点について『タリン2』は、国際法上それを禁じる規則はないと結論づけた（規則32）。第2に、諜報が国際法上、主権侵害など違法な方法で行われた場合、全体として諜報行為が違法とみなされる。ただし、何が主権侵害に相当するのか、という問題の捉え方によって、第2の点に関する判断は変わり得る。（特段の物理的被害が発生しないという意味で）単なるハッキングは、主権侵害にさえ該当しないという『タリン2』の多数説は、実はエストニア（2009年来、国連のサイバーGGEの一員）など一部の国にも既に共有されているが、サイバー諜報に関心を寄せる各国政府にとっても受け入れやすい考えとも言える。『タリン2』を読むと、本質的な政府の機能に分類されるネットワークに侵入する場合（前述の、米韓両軍による対北朝鮮攻撃計画データの窃取）はおしなべて主権侵害とみなされうるものの、そうではない場合、例えば、本質的な政府の機能を構成しない組織や産業インフラに対するハッキングおよび情報の窃取は、方法という観点からも違法とならないという帰結が示唆される。他方、主権侵害の認定基準が、本質的な政府の機能の侵害ということであれば、本国と在外公館との間の電子的通信の傍受は、常に主権侵害に該当する。公用通信の不可侵については、1961年外交関係に関するウィーン条約でも定められている通りだが、『タリン2』はこの規則がサイバー通信にも適用されるとしている（規則41）。サイバー公用通信は場所のいかんを問わず不可侵であり、仮に傍受を行う国の領域内に置かれたインフラを経由した場合であっても、この傍受は違法である。もっとも、方法において違法であるからと言って、各国がサイバー諜報の実施を躊躇し、中断するか否かは、また別の問題である。

おわりに

国家間のサイバー攻撃は今日、世界中で日常的に行われているが、関係当事国は必ずしもその国際法上の正当性を明らかにしているわけではない。こうした状況を背景として、武力攻撃未満のサイバー攻撃に関する国際法を明文化した『タリン2』には一定の有用性が認められる。他方、『タリン』および『タリン2』の双方とも、一部、立法論的な記述（特に武力行使の認定基準）や未解決の論点も含んでいることには留意しなければならない。さらに、専門家らの多数説として提示された内容であっても、機械的に適用するのは

禁物である。一口に DDoS 攻撃と言っても、エストニアと北朝鮮とでは、本質的な政府の機能がサイバー・インフラに依存する度合いは異なるため、その被害の程度も著しく異なることが予想される。そうした事実に即した判断も含め、国家のとるサイバー活動については国際法上合法か否かの見極めが今後求められ、『タリン 2』はその際の 1 つの手がかりを提供するものと思われる。

参考文献

•Terry D. Gill, "Non-Intervention in the Cyber Context," in Katharina Ziolkowski, ed., Peacetime Regime for State Activities in Cyberspace (NATO CCD COE, 2013), pp. 217-238.

• Marina Kaljurand, "United Nations Group of Governmental Experts: The Estonian Perspective," in Anna-Maria Osula and Henry Rõigas, eds., International Cyber Norms: Legal, Policy & Industry Perspectives (NATO CCD COE, 2016), Chapter 6.

• Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017)

(2017 年 10 月 20 日脱稿)

ブリーフィング・メモに関するご意見・ご質問等は、防衛研究所企画部企画調整課までお寄せ下さい。

防衛研究所企画部企画調整課

外　線：０３－３２６０－３０１１　　専用線：８－６－２９１７１

ＦＡＸ：０３－３２６０－３０３４　　※防衛研究所ウェブサイト：http://www.nids.mod.go.jp