サイバー攻撃、経済安全保障と国際法

2025.6.27　　中谷和弘@CSTIA

1. タリン・マニュアルについて

私は、2015 年から 2016 年にかけて欧州エストニアの首都タリンにある NATO サイバー防衛センター（Cooperative Cyber Defence Centre of Excellence, CCD COE）において作業がなされたタリン・マニュアル 2.0 の作成に 17 名の法律専門家の一員として関与した。エストニアは E-stonia と呼ばれるほど電子化が進んだ国家であるが、2007 年にロシアから大規模なサイバー攻撃を受けて政府機能が麻痺した。そのエストニアにおいて CCD COE が設置され、そのプロジェクトとしてなされた。

タリン・マニュアルは、法律専門家が個人的資格で集まって、サイバー攻撃に関する国際法のルールをコメンタリーとともに記述したものである。この作業は、米国海軍大学校の Michael Schmitt 教授を中心にすすめられ、まず 95 の規則とコメンタリーからなる「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」(Tallinn Manual on the International law Applicable to Cyber Warfare) がまとめられ、2013 年 4 月に Cambridge University Press から刊行された。後にタリン・マニュアル 1.0 と呼ばれるようになったこのマニュアルは、第 1 部「国際サイバー安全保障法」及び第 2 部「サイバー武力紛争法」からなり、これらは「有事・戦時」を対象にしたものである。その後、さらに「平時」におけるルールにつき検討がなされ、「サイバー行動に適用される国際法に関するタリン・マニュアル 2.0」(Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations) がまとめられ、2017 年 2 月に同じく Cambridge University Press から刊行された。

タリン・マニュアル 2.0 は 154 の規則とコメンタリーからなり、第 1 部「一般国際法とサイバー空間」、第 2 部「国際法の特別の体制とサイバー空間」、第 3 部「国際の平和及び安全とサイバー活動」、第 4 部「サイバー武力紛争法」から構成されている。第 3 部の一部と第 4 部はタリン・マニュアル 1.0 をほぼそのまま取り入れている。

私自身は、legal experts の 1 人としてタリン・マニュアル 2.0 の作成に関与し、2015 年から 2016 年にかけて 3 回にわたり各 1 週間開催されたタリンでの会議に参加した。英語の原著は 598 頁からなる大部のものであり、相当複雑な議論も展開されているため、各規則の訳とコメンタリーの要旨を日本の読者にわかりやすく示す必要があると感じ、河野桂子氏(防衛研究所、現在、NATO CCD COE)及び黒﨑将広氏(防衛大学校）とともに『サイバー攻撃の国際法　タリン・マニュアル 2.0 の解説』を 2018 年 4 月に信山社から刊行した。

タリン・マニュアルは、サイバー攻撃に関する国際法ルールを「作成」したり「提案」したりするものではない。既存の慣習国際法（国際社会のすべての国家に等しく適用される不文法）がサイバー空間にも適用されるという前提（これは西側先進諸国を中心とする少なからぬ諸国家の基本的立場でもある）の下に、サイバー攻撃に適用される慣習国際法を明文化し、コメンタリーとともに記述するという作業である。Pablo Picasso は“I do not seek, I find.” と言ったが、まさに慣習国際法を「発見」するという地味だが重要かつ容易ではない作業である。

タリン・マニュアル自体は民間のものであるが、西側諸国をはじめとする多くの国家の共通認識とほぼ一致しており、国際社会において一定の権威を獲得している。

タリン・マニュアル 2.0 は、次の 20 項目から構成されている。第 1 部「一般国際法とサ

イバー空間」（General International Law and Cyberspace)は、1. 主権(Sovereignty,規則 1 〜5)、2.相当の注意(Due Diligence, 規則 6〜7)、3.管轄権（Jurisdiction、規則 8〜13)、4.国家責任法（Law of International Responsibility, 規則 14〜31)、5.それ自体は国際法によって規律されないサイバー行動（Cyber Operations not per se Regulated by International Law, 規則 32〜33) からなる。第 2 部「国際法の特別の体制とサイバー空間」(Specialized Regimes of International law and Cyberspace) は、6.国際人権法(International Human Rights Law, 規則 34〜38)、7.外交及び領事法(Diplomatic and Consular Law, 規則 39〜44)、8.海洋法（Law of the Sea, 規則 45〜54)、9.航空法(Air Law, 規則 55〜57)、10.宇宙法(Space Law, 規則 58〜60)、11. 国際電気通信法(International Telecommunication Law, 規則 61〜64)かならなる。第 3 部「国際の平和及び安全とサイバー活動」(International Peace and Security and Cyber Activities) は、12.平和的解決（Peaceful Settlement,, 規則 65)、13.干渉の禁止（Prohibition of Intervention, 規則 66〜67)、14.武力の行使(Use of Force, 規則 68〜75)、15.集団的安全保障(Collective Security, 規則 76〜79)からなる。 第 4 部「サイバー武力紛争法」(The Law of Cyber Armed Conflict)は、16. 武力紛争法一般(The Law of Armed Conflict Generally, 規則 80〜85)、17. 敵対行為の遂行(Conduct of Hostilities, 規則 86〜130)、18. 特定の人、物及び活動(Certain Persons,Objects,and Activities, 規則 131〜145)、19. 占領(Occupation、規則 146〜149)、20.中立(Neutrality, 規則 151〜154)からなる。

タリン・マニュアル 2.0 は、サイバー攻撃が各分野の国際法ルールとの関連でどう位置づけられるかを包括的に検討した成果であり、サイバー攻撃という観点から国際法全般を鳥瞰するものとなっている。

ここでは、以下、タリン・マニュアル 2.0 の主な内容について概観することにしたい。

第 1 に、サイバー攻撃の定義について。規則 92 は、「サイバー攻撃とは、攻撃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、又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行動である」と規定する。データへの攻撃を目的とするサイバー行動も、個人の死傷や物体の損壊・破壊をもたらすことが予見可能である場合にはサイバー攻撃となる。

第 2 に、主権侵害と干渉について。規則 4 は、「国家は、他国の主権を侵害するサイバー行動を行ってはならない」と規定する。領域外からのサイバー行動については、サイバー・インフラの物理的損害が発生した場合のみならず機能の喪失が生じた場合も主権侵害となる。政府機能の行使に必要なデータの改変・削除も主権侵害となる。干渉の禁止については、規則 66 は、「国家は、他国の国内又は対外事項に、サイバー手段による場合も含め、干渉してはならない」と規定する。ここで禁止される干渉とは国家が自己決定できる事項（国内管轄事項）に対して強制を伴う介入をすることである。

第 3 に、武力攻撃と自衛について。一定以上の「規模及び効果」を有するサイバー攻撃は国際法上の「武力攻撃」に該当する。その場合には、武力攻撃を受けた国は個別的自衛権の発動が、その友好・同盟国は集団的自衛権の発動が可能となる。規則 71 は、「武力攻撃の水準に至るサイバー行動の目標となる国家は、固有の自衛権を行使することができる。サイバー行動が武力攻撃に該当するか否かは、その規模及び効果による」と規定する。多数の人間を殺傷したり、財産に重大な損害・破壊をもたらすサイバー行動は、武力攻撃に必要な規模及び効果を有する。自衛権の発動としての措置は、サイバー手段によるものと非サイバー手段によるものの双方が想定される。個別的自衛権の行使には、「必要性と均衡性」（規則 72）及び「急迫性と即時性」（規則 73)の要件を満たす必要があり、集団的

自衛権の行使にはさらに「被害国の要請」（規則 74）の要件も満たす必要がある。なお、テロリスト等の非国家主体によるサイバー攻撃も武力攻撃の主体になりうるため、これに対して自衛権の行使が可能というのが、legal experts の多数意見である。但し、主権原則を規定する上記の規則 4 との関連で、自衛権が行使できるのは、非国家主体の所在地国の同意がある場合か、所在地国が武力攻撃に効果的に対応する意思又は能力を欠いている場合に限られる。先制的自衛については、実行可能な最後の防衛の機会だと考えられる場合には認められるという見解が多数意見であった。

第 4 に、国際法上違法な（但し武力攻撃には至らない程度の）サイバー攻撃に対しては、被害国は対抗措置（countermeasures) をとりうる。規則 20 は、「国家は、他国が自国に対して負う国際法上の義務違反への反応として、対抗措置（性質上サイバーであるか否かを問わない）をとる権限を有する」と規定する。対抗措置には、サイバー手段によるものも想定され得るが、現実には対抗措置の中心をなすのは経済的措置である。サイバー攻撃が発生した場合に被害国がとる反応で現実に採用かつ公表されているものは、サイバー手段による反撃ではなく、経済的な措置（特にサイバー攻撃に責任を有する個人や団体の金融資産の凍結）である。なお、外交上の措置（相手国の外交官・領事官の追放や大使館・領事館の閉鎖命令、自国の外交官・領事官の召喚や大使館・領事館の閉鎖など）も経済的措置と同様にサイバー攻撃への反応として発動されるが、こういった外交上の措置は非友好的であってもそれ自体裁量的にとりうる報復（retorsion）であって、対抗措置とは国際法上区別される。対抗措置が容認される（＝違法性が阻却される）ためには、均衡性（規則 23）をはじめとする要件を満たす必要がある。規則 24 は、「被害国のみが対抗措置（性質上サイバーであるか否かを問わない）をとることができる」と規定する。対抗措置をとることができるのは国家のみであり、例えばサイバー攻撃を受けた企業自らが対抗措置をとることはできない。また、直接の被害国以外の第三国が対抗措置をとることは通常はできない。

第 5 に、国家機関によるサイバー攻撃について。規則 15 は、「国家機関又は国内法によって統治権能の一部を行使する権限を付与された個人若しくは団体によってなされたサイバー行動は、当該国に帰属する」と規定する。法令や契約によって他国にサイバー攻撃を行う法的権限を付与された企業の行動も、国家に責任が帰属する。企業が権限を逸脱してハック・バックをした場合にも、その行為は国家に帰属する。なお、ゾンビ・コンピュータによる DDos 攻撃のような場合もあるため、ある国家のサイバー・インフラからサイバー攻撃がなされたからという事実だけでは、当該国に責任が帰属するという証拠としては不十分である。

第 6 に、私人等の非国家主体によるサイバー攻撃について。規則 17 は、「非国家主体によってなされたサイバー行動は、次の場合に国家に帰属する。(a) その指示に従い又はその指揮若しくは命令下でなされた場合、又は(b)国家が当該活動を自己の活動として認め、かつ採用した場合」と規定する。非国家主体には、個人のハッカー、ハッカー集団、サイバー犯罪組織、IT 関連企業、サイバー・テロリスト、反政府勢力等が含まれる。なお、(a)又は(b)に該当しない場合には、国家は私人によるサイバー攻撃に関して一切の責任を負わない訳ではなく、次に見る相当の注意を欠いていた場合には、結果として責任を負うことになる。国際法の国家責任のルールに従い、私人によるサイバー攻撃に対しては、私人の本国や領域国には直接国家責任は帰属しないが、相当の注意義務を欠いたために損害が生じた場合には、相当の注意義務の不作為ゆえに結果として当該国に国家責任が生じることになる。

第 7 に、相当の注意と経由国の責任について。規則 6 は、「国家は、自国の領域又は自国の政府の支配下にある領域若しくはサイバー・インフラが、他国の権利に影響を与え重大で有害な結果を生じるサイバー行動のために使用されることを許さないよう、相当の注意を払わなければならない」と規定する。規則 7 は、「相当の注意義務は、他国の権利に影響を与え重大で有害な結果を生じるサイバー行動を終了させるために、国家が当該状況において実行可能なすべての措置をとることを要求する」と規定する。相当の注意義務の程度は、先進国と途上国では異なり得る。経由国の責任に関しては、規則 6 のコメンタリーでは、A 国に所在するハッカー集団が C 国にあるサイバー施設を使って B 国に対するサイバー攻撃を実施したが、C 国はそれを知りながら攻撃を終了させるため実行可能な措置をとらなかった場合には、C 国は相当の注意原則の違反になるとする。これに対して、例えばデータが通過するだけの国家が相当の注意義務を負うかについては、サイバー行動を了知し、かつそれを終了させるため実行可能な措置をとれる場合には、相当の注意義務を負うが、通過国は一般には悪意あるトラフィックを了知しえないので、相当の注意義務を負う場合は現実には例外的になると考えられる。

第 8 に、サイバー諜報（cyber espionage）について。「5. それ自体は国際法によって規律されないサイバー行動」は、サイバー諜報を念頭においている。規則 32 は、「国家による平時のサイバー諜報はそれ自体は国際法に違反しないが、それを遂行する方法は国際法違反となりうる」と規定する。諜報（スパイ行為）一般は、国際法上、禁止はされていないが、各国の国内法で刑事罰を課すことは可能という独自の法的性質を有している。サイバー諜報についても基本的に同様であり、サイバー諜報それ自体は国際法違反とはいえないが、行動によっては例えば干渉という国際法違反になることがある。

第 9 に、サイバー通信の停止について。規則 62 では、「(a) 国家は、部分的又は完全に、自国領域内における国際サイバー通信業務を停止することができる。当該停止の即時の通知が他国に対してなされなぇればならない。(b) 国家は、国内法令、公の秩序若しくは善良の風俗に反すると認められ、又は国家の安全にとって危険である私用のサイバー通信の伝達を停止することができる」と規定する。この規定は、国際電気通信連合（ITU）憲章 35 条及び 34 条 2 項に基づくものである。2011 年のアラブの春のように反体制運動が SNS で広まった際に国家がサイバー通信を停止することは、国際電気通信法の下では国家の権利であるが、規則 35「個人は、サイバー関連活動に関し、他で享受するのと同じ国際人権を有する」には違反する可能性があることに留意する必要がある。

第 10 に、軍事目標主義について。規則 99 は、「民用物はサイバー攻撃の対象とされてはならない。コンピュータ、コンピュータ・ネットワーク及びサイバー・インフラは、それらが軍事目標である場合にはサイバー攻撃の対象となる」と規定する。規則 100 は、「民用物は、軍事目標ではないすべての物をいう。軍事目標は、その性質、位置、用途又は使用が軍事活動に効果的に資するものであってその全面的又は部分的な破壊、奪取又は無効化が、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をいう。軍事目標はコンピュータ、コンピュータ・ネットワーク及びサイバー・インフラを含みうる」と規定する。武力紛争法の基本原則の 1 つである軍事目標主義は、1949 年ジュネーヴ条約第 1 追加議定書 52 条でも規定されており、タリン・マニュアルでも採用されている。なお、民生及び軍事の両用に使用される物については、規則 101 が、「民用及び軍事の双方の目的に使用される物（コンピュータ、コンピュータ・ネットワーク及びサイバー・インフラを含む）は、軍事目標である」と規定する。

タリン・マニュアルは、個人的資格でタリンに集った有識者が考えるサイバー攻撃に関する国際法にとどまるものであるが、他に包括的にサイバー攻撃に関する国際法ルールを提示したものもない所から、国際社会において既に一定の権威を有する文書になっている。legal experts は、各国政府や国際組織が参照・引用してくれることを期待しつつ、タリン・マニュアルを作成した。但し、タリン・マニュアル 2.0 が公表されてから 8 年経つが、諸国家の反応は未だ様子見といった所である。諸国家としては、サイバー攻撃をめぐる状況がどう推移するか不明確な現状において、「規則〇〇は慣習国際法になっているが、規則 XX は慣習国際法になっていない」といった何らかの見解を表明することが、将来自国にとって不利な証拠となることを恐れて慎重になっているのかもしれない。

勿論、タリン・マニュアルは万能のものではない。タリン・マニュアルはサイバー攻撃に関する詳細な実体ルールを示したが、現実に最初に問題となる「誰がサイバー攻撃をしたか」をはっきりさせるのに必要な事実認定の機関は国際社会には存在せず、また事実認定と証拠に関する手続ルールはタリン・マニュアルの射程範囲外である。有責者の確定にあたっては、立証の程度を従来の国際裁判で用いられてきた一般的基準よりもゆるやかなものにしないと、およそ立証が困難になるといった指摘もなされている。

２．サイバー攻撃対処のための国家間の合意

サイバー攻撃に対処するためには、さらに、信頼醸成措置（Confidence Building Measures）や能力構築措置（Capacity Building Measures）も重要である。信頼醸成措置は冷戦下の米国・ソ連間及び西側諸国・東側諸国間の一連の合意(米ソホットライン協定、米ソ核戦争防止協定、米ソ公海事故防止協定、欧州安全保障協力会議ヘルシンキ最終議定書など）を端緒とするものであり、潜在的な敵対国との間での緊張緩和や緊急時対応等を内容とするものである。サイバー分野での信頼醸成措置として、米国とロシアが 2013 年 6 月 17 日に「情報・通信技術の安全に関する協力」（Cooperation on Information and Communications Technology Security）という合意文書を取り交わしたことが注目される。同文書において、米ロは、①Computer Emergency Response Teams (CERT) 間のリンク、②核リスク減少センターを通じての通報の交換、③ホワイトハウス・クレムリン間の直接コミュニケーション・ラインの創設、の３点で合意した。また、米国と中国は、2015 年 9 月 25 日に、両国は知的財産権のサイバー窃盗を行ったり知りながらサポートしたりしないことで合意した（同年秋の G20 アンタルヤ・サミットでの首脳コミュニケにおいても同様の合意がなされた）。ロシアと中国は、2015 年 4 月 30 日に、互いにサイバー攻撃を行わないことで合意した。信頼醸成措置は、意図的なサイバー攻撃には無力かもしれないが、偶発的なサイバー攻撃を予防し、また損害を小さくするためには一定の効果を有し得るものである。

G7 では、2017 年 6 月のイタリアでのサミットの際に「サイバー空間における責任ある国家の行動に関するＧ７ルッカ宣言」が採択されたことが注目される。とりわけ、「国家は，その領域が情報通信技術を利用した国際違法行為に利用されることを了知しながら許すべきではない」、「国家は，国際法に基づく義務に反して，故意に重要インフラに損害を与える又は公共サービスを提供する重要インフラの利用及び運用を害する情報通信技術活動を実施し，又はそれを了知しながら支援すべきではない」と宣言されたことが国際法上は意義深い。

2021 年 5 月にはサイバーセキュリティに関する国連政府専門家会合（GGE）において「サ

イバー空間における責任ある国家の行動に関する報告書」が採択された。同年 12 月の国連総会決議では、各加盟国はこれに従うよう勧告がなされた。注目すべき規定として、規範 13C「国は、情報通信技術を用いた国際違法行為のために自国の領域を知りながら使用を許容すべきではない」との規定がある。

G7 の合意や GGE 報告書は政治的にはタリン・マニュアルよりも重要であるが、内容は概して薄い。これは諸国家の最大公約数にとどまるからである（特に GGE の場合、西側諸国の見解と中露の見解の一致がないとまとまらない）。国際法上の諸課題の解決により資するのはタリン・マニュアルである。

３．サイバー攻撃対処条約は必要か

サイバー攻撃対処条約は必要であろうか。西側諸国の見解は、既にサイバー攻撃に関する慣習国際法が存在するから新たな条約は不要というものである。これに対して、中国やロシアや一部の途上国の見解は、必要というものである。但し、ここには裏があることに注意しなければならない。後者の諸国がサイバー活動について最も恐れているのは、アラブの春の再現（反体制活動が SNS を通じて広まること）であり、新たな条約には情報の国家統制条項を入れことを最重要視していることである。これに対して、西側諸国の見解は表現の自由、情報の自由を最重要視している。もし国連総会でサイバー攻撃対処条約が議論されるとなると、多数派を占めるのは途上国であり、その多くは非民主主義国家であるため、情報の国家統制条項が入ってしまう可能性が高い。さらに、条約作成には長年を要する上、サイバー攻撃を行っていると疑われる肝心の国家は条約に入らないかもしれない。「既に慣習国際法は存在し、適用できる以上、新たな条約は不要」という西側諸国の見解は、こうした裏事情まで勘案すると、合理的であることがわかる。そして、慣習国際法を同定する際に最も有用な指針となるのが、まさにこのタリン・マニュアルなのである。この意味で、タリン・マニュアルはサイバー空間における「法の支配」に大きな貢献をしたものといえよう。

４．サイバー諜報について

先ほど申し上げたように、スパイ（諜報、espionage）は、第１に、国際法上、包括的にそれを違法とするルールはないが、諜報の態様によっては、主権侵害や内政干渉になって国際法違反となることがある、第２に、各国が反スパイ法という国内法を制定してペナルティーを科すことはその国の自由である、という特異な法構造にある。日本のように反スパイ法のない国家は自らを不利な立場においていることを自覚すべきである。なお、英国は
サイバー攻撃は主権侵害の問題を生じないという独自の立場をとっている。その理由は明らかではないが、ファイブアイズのような活動に鑑みて、サイバー諜報を容易にするためあえてそのような解釈をとっているのかもしれない。

サイバー諜報（cyber espionage）についても同様のことがいえる。サイバー諜報はサイバー攻撃の一種であるが、強いて区別するのであれば、狭義のサイバー諜報とは、機密情報の盗視やコピーはするが、改竄や窃取はしない（まして重要インフラの破壊・暴発などはしない）ということになろう。

やや独自の扱いを要するのがサイバー経済諜報（economic cyber espionage）である。企業の機密情報を盗視・複写・改竄するサイバー経済諜報は、国家の機密情報の諜報の場合と比べて主権侵害や内政干渉になる可能性が一般には低い。それでは国際法上は違法でないかというとそうではない。経済サイバー諜報は WTO の TRIPS 協定（貿易関連知的所有権協定）39 条で規定された「開示されていない情報の保護」に違反すると解せられる。そうである以上、WTO の紛争処理機関（パネル、上級委員会）に訴えることが可能である。まだそのような付託の例はないが、日本企業が国外から経済サイバー諜報を受けた場合への日本政府による対応として、WTO 付託が首尾よく行くように法的な準備しておくことが重要である。

サイバー諜報が外交関係断絶に至った例もある。2021 年 8 月 24 日にアルジェリアがモロッコとの外交関係を断絶した。アルジェリアは、西サハラをめぐる長年に亘るモロッコとの対立を背景にして、モロッコの情報機関がイスラエルのサイバー企業 NSO Group が開発したスパイウエア Pegasus を使ってアルジェリア当局を諜報していたと主張して、モロッコとの外交関係断絶に至ったのであった。これはサイバー諜報が外交関係断絶に至った初のケースとして注目される。なお、アルバニアは 2022 年 7 月にイランからサイバー攻撃を受けたとして、同年 9 月 7 日にイランとの外交関係を断絶した。サイバー攻撃が外交関係断絶に至った初のケースとして注目される。

5. 能動的サイバーディフェンスについて

「サイバー攻撃は攻撃者に有利である」としばしば指摘される。その主な理由は、第１に攻撃元を特定できるか、第２に国家への責任帰属が可能かという２つの意味でのアトリビューション（帰属）が困難だからである。

第１のアトリビューションは「事実としてのアトリビューション」とも呼ばれるが、サイバー攻撃元を特定することは技術的におよそ容易ではない。被害国の側に実空間での被害と同程度の立証責任を負わせるとなると立証は著しく困難になりかねない。

第２のアトリビューションは「法的なアトリビューション」とも呼ばれるが、たとえ攻撃元を特定できたとしても、国家に責任が帰属することを立証することは法的に容易ではない。この点に関しては、私人の行為の国家への責任帰属のルールなど国際法における国家責任のルールが適用されることになる。国家への責任帰属の要件について、より厳格な要件である「実効的コントロール」まで課す必要があるのか、より緩やかな要件である「全般的コントロール」で良いのかについて議論がある。前者の基準では立証は極めて困難になりかねない。

サイバー攻撃の対象は様々であるが、最も深刻なのは重要インフラ（原発、ダム、航空管制など）に対する攻撃であろう。国家・企業・個人の重要情報の盗取や改竄も深刻な攻撃であるし、選挙妨害も主権侵害や内政干渉となりうる深刻な攻撃である。

サイバー攻撃がなされて原発が暴発し、ダムが決壊し、航空管制が無力化して航空機事故が発生し、国家・企業・個人の重要情報の盗取や改竄がなされ、選挙干渉がなされてから対処するのでは遅すぎる。国家と国民の利益を守るためには、サイバー攻撃がなされる前の段階で適切な対処をして防止することが何よりも重要である。まさに能動的サイバーディフェンスが必要とされる所以である。

能動的サイバーディフェンスの確立した定義がないと思われるが、「サイバー攻撃やそ

の恐れに対して、攻撃者のサーバーへの侵入やマルウェアの削除等を行うことで攻撃を無害化したり阻止したりすること」と一応は定義できる。

能動的サイバーディフェンスの射程範囲をどう考えるか。一方の局にはいわゆるハックバック（サイバー手段による反撃）がある。国際法上はハックバックも自衛や対抗措置などの要件を満たせば認められ得る。但し諸国家はハックバックしたとは公言しない。手の内をさらすことになりかねないからである。武力攻撃に該当するサイバー攻撃に対しては自衛権を、国際法違反のサイバー攻撃に対しては対抗措置をとることが認められ、これらにはサイバー手段、非サイバー手段の双方が含まれ得る。他方の極には、国家が裁量的に発動できる措置がある。例えばハニーポット（サイバー手段によるおとり）を設定して罠にはめることは、国際法上は裁量的にとりうる。両者の中間には、様々な能動的サイバーディフェンスの措置が存在する。

なお、国家安全保障戦略においては、「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」としているため、武力攻撃に対する自衛権の発動としてのサイバー行動は射程範囲外である。

6. 能動的サイバーディフェンスの国際法上の正当化根拠としての緊急避難

国連国際法委員会が 2001 年にまとめた「国家責任条文」20 条～25 条が示すように、国際法上は、違法性阻却事由（国際法違反ではなくなり正当化される特別の理由）に該当するのは、自衛、対抗措置、緊急避難、同意、不可抗力、遭難の６つである。能動的サイバーディフェンスが、通常であれば相手国の主権侵害などの国際法違反を生じさせてしまう場合がたとえ存在するとしても、これらの事由のいずれかに該当すれば、国際法上正当化され、国際法違反の責任を負うことはなくなる。

能動的サイバーディフェンスの正当化根拠として考えられるのが、「対抗措置」と「緊急避難」である。私としては「緊急措置」がより良いと考える。

「対抗措置」(countermeasures)は、相手国の国際法違反への反応（基本的に経済分野を中心とした非軍事分野での反応）であり、均衡性のとれた措置をとることが認められる。但し、対抗措置の援用には、まず国際法違反の存在を立証することが必要となる。この立証は、現実には前述の２つのアトリビューションの困難に直面することになりかねない。また先制対抗措置は一般には容認しがたいため、サイバー攻撃発生前に対抗措置として ACD を発動することは国際法上は困難である。

「緊急避難」(necessity) は、能動的サイバーディフェンスの国際法上の正当化根拠としてより使い勝手の良いものである。緊急避難は相手国の国際法違反を前提にしないため、2 つのアトリビューションの困難に直面することはない。当該行為が「重大かつ差し迫った危険から根本的利益を守るために当該国にとって唯一の方法であること」を立証すれば良い。「国家責任条文」25 条 1 項は、「国は、次の場合を除くほか、自国の国際義務に合致しない行為の違法性を阻却する根拠として緊急避難を援用することができない。(a)当該行為が、重大かつ差し迫った危険から根本的利益を守るために当該国にとって唯一の方法であり、かつ、(b) 当該行為が、その義務の相手国又は国際社会全体の根本的利益を大きく損なうものではないこと。」と規定する。つまり援用国自身にとっての必要性をきちんと

主張できれば良い。緊急避難としてとる措置の内容は「義務の相手国又は国際社会全体の根本的利益を大きく損なうもの」は認められないが、サイバー能力の無力化はおよそそれには該当しない。

タリン・マニュアルの規則 4 では、「国家は、他国の主権を侵害するサイバー行動を行ってはならない」と規定する。コメンタリーでは次のように指摘する。①ある国家の機関が他国領域内に物理的に存在する間にサイバー行動をとることは、当該国の主権侵害となる（例．他国領域内のインフラに USB メモリを使ってマルウェアを感染させる）。
②他国領域内でのサイバー諜報も主権侵害となる場合がある。③領域外からの無線信号に対する単なる妨害は主権侵害にはあたらない。④本質的な政府の権能の行使に必要なデータやサービスを妨げるサイバー行動（社会保障、選挙、徴税、外交、国防に関するデータの改変・削除）は主権の侵害となる。

規則 26 では、「国家は、根本的な利益に対する重大で差し迫った危険を示す行為への反応として、そうすることが当該利益を守る唯一の手段である場合には、緊急避難を理由として行動することができる」と規定する。コメンタリーでは、「緊急避難は、銀行システム、証券取引所、航空機の離発着、年金などの社会福祉 制度の運用中断、国民の健康を危険にさらす情報の改竄、環境損害の発生、配電網 の遮断、国の食料配給網や防空システムの無力化などに加えて、国の安全保障、経済、公衆衛生、治安又は環境に関係する重要インフラに深刻な被害が生じた場合に援用できる」と指摘する。また、「サイバー攻撃の発生源が不明な場合でも、被害国は状況及び潜在的な救済措置を評価する間、緊急避難に基づきサイバーインフラを遮断することができる。また被害国は緊急避難に基づきハックバックを行うことも正当化されうる」と指摘する。

以上より、能動的サイバーディフェンスは緊急避難で十分正当化できるため、国際法上は能動的サイバーディフェンスの合法性について特に心配する要因はない。

以上に関連して、有識者提言においても、「対抗措置については、相手国の先行する違法行 為の存在や被害の程度との均衡性を証明しなければならないなどの点を踏まえると、実務上、 援用する違法性阻却事由としては、緊急状態の方が援用しやすい」という妥当な指摘を行っている。

残念なことに日本のサイバーセキュリティの対応は先進的とは言えなかった。2021 年に英国の国際問題戦略研究所（IISS）が発表した各国のサイバー能力についての報告書では、日本は第 3 グループ（優良可でいえば可）となってしまった。通信の秘密の過剰な保護がリスクになっている旨も指摘されている。我が国においては、国際標準に合致した国内法対応が早急に求められる。サイバー攻撃においては、ボットネットに代表されるように、ある国が攻撃を受けると他国にも影響が及びかねない。日本がサイバー攻撃の「ぬけ穴」になってはいけない。万全のサイバー対応をすることは「国際社会における法の支配」への貢献にとっても不可欠である。

なお、本年成立した「重要電子計算機に対する不正な行為による被害の防止に関する法律」では、78 条において「この法律の施行に当たっては、我が国が締結した条約その他の国際約束の誠実な履行を妨げることがないよう留意しなければならない」との規定が念のためにおかれており、元々慎重な日本政府が active cyber defense において国際法に違背する心配はないといえる。自衛隊法には 81 条の 3（重要電子計算機に対する通信防護措置）が、警察官職務執行法には 6 条の 2（サイバー危害防止措置執行官による措置）が新設され、自衛隊や警察が必要な措置をとれることになった。

さらに、タリン・マニュアルの規則７は、「国家は、自国の領域又は自国の政府の支配下にある領域若しくはサイバー・インフラが、他国の権利に影響を与え重大で有害な結果を生じるサイバー行動のために使用されることを許さないよう、相当の注意を払わなければならない」と規定する。能動的サイバーディフェンスをもし全く行わないとなると「相当の注意義務」の欠如とみなされかねないことにも留意する必要がある。

能動的サイバーディフェンスによってサイバー攻撃やサイバー諜報から国家と国民を防衛する体制を整えておかないと、サイバー犯罪に関する国際共同捜査を含む国際協調行動をとる上での大きな障害になりかねない。サイバー分野での国際協力がうまく行くためには，参加各国が一定以上のサイバー能力を有し，かつ機密情報を提供できることが当然の前提である。

さらに，一国に対するサイバー攻撃の悪影響は当該国内にとどまるものではなく，他国にも悪影響が及びことが不可避であることに鑑みると，サイバー攻撃を予防するために能動的サイバーディフェンスを行うことは，国際社会に対する責務といっても過言ではない。「国際社会における法の支配」を重視する我が国としては，サイバー分野においても責任ある行動をとることが必須であり，その中には関連する国内法の整備も当然に含まれる。

「重要電子計算機に対する不正な行為による被害の防止に関する法律」では、監視対象として「外外通信」、「内外通信」、「外内通信」が挙げられている。他方、「内内通信」は対象外である。懸念されるのは、国内通信事業者が外国勢力の支配・影響下におかれてしまった場合の対応である。電気通信事業法は、1997 年の WTO 自由化約束を経て、同年の改正により外資規制（旧第一種電気通信事業者[電気通信回線設備を設置してサービス提供する事業者]を対象）を撤廃したため、復活は困難（一定規模以上の複数の電気通信事業者に外資規制 を設ける場合、同様の留保が可能か否かについて、数年を要する可能性のある国際交渉が必要となる）。外国勢力による土地購入についても WTO,GATS に加入する際に日本は何ら制限をしなかったため、事後的に規制をするのが著しく困難になってしまっている。「自由化一本打法」であって経済安全保障についての配慮を欠くものであったことが悔やまれる。外為法による外資規制のみで外国勢力による国内通信事業者への影響力行使に完全に対応できるだろうか。

また、外国の政府や企業が日本の政府や企業に対してサイバー攻撃やサイバー諜報を行った場合に、当該政府や企業の有責者の資産を凍結し、入国を拒否するという経済制裁措置をとる万全の法体制を整えておくことも重要である。諸国家はサイバー手段で反撃したとは（たとえやっていても）公言せず、公言するのは、有責者の資産凍結や入国禁止である。外為法では、10 条 1 項の閣議決定が行われたときには、我が国の単独の判断で有責者の資産凍結を行うことができると規定する（16 条 1 項）。閣議決定が確実かつ迅速になされる必要がある。有責者の入国禁止については，出入国管理及び難民認定法５条１項 において列挙された上陸　拒否事由のうち該当すると思われるのは，14 号の「公安条項」である（2020 年のコロナの際に感染者が乗船していたオランダの客船の入港を拒否した）。有責者の入国拒否が円滑にできるようにしておくことが重要である。

７．ランサムウェア攻撃に対する身代金の支払をめぐって

ランサムウェアとは、「感染するとパソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不

正プログラム」であり、サイバー攻撃の主要な一態様である。日本における 2024 年のランサムウェアの被害報告件数は 222 件。

ここでは代表的なランサムウェア攻撃として Colonial Pipeline 事件をとりあげる。2001 年 5 月 7 日に発生。バイデン大統領は 5 月 9 日に緊急事態を宣言し、米国内での石油輸送量の上限規制を一時的に停止した。5 月 10 日には連邦捜査局（FBI）は Darkside という集団の犯行であるとした。同日、ジョージア州知事も同州の緊急事態を宣言した。バイデン大統領は 5 月 12 日にサイバーセキュリティを強化する大統領令 14028 を発した。同日、パイプラインの操業が再開された。CEO の Joseph Burount は、「440 万ドルの身代金の支払をしたことは国家のために正しいことであった」と発言した。司法省は 6 月 7 日に支払われた身代金のうち約半分の 63.7 ビットコイン分（約 230 万ドル）を押収したと発表した。

ロシア政府や北朝鮮政府はランサムウェア攻撃に関与してきたとされる。とりわけランサムウェア攻撃によって資金を獲得してきたのが北朝鮮である。国連の対北朝鮮制裁専門家パネルの最終報告書（2024 年 3 月 7 日公表）は、北朝鮮が関与する Lazarus Group によるランサムウェア攻撃により 700 以上の被害者から 260 万ドルの身代金を徴収した旨、指摘する。米サイバー軍前司令官のポール・ナカソネは、北朝鮮の GDP の約 4 分の 1 がランサムウェア攻撃によって得られていると述べている。

国際カウンターランサムウェア・イニシアティブ（The International Counter Ransomware Initiative, CRI）は、ランサムウエアに対抗するための国際的なプラットフォームであり、一国や一組織のみではランサムウェアに実効的に対処できず、国際的なパートナーシップがランサムウェアの実行者とそのエコシステムに対抗する強い戦力となるして、2021 年に創設された。2024 年 5 月 8 日時点でのメンバーは、67 国（米国、日本、英国、フランス、イタリア、カナダ、オーストラリア、ブラジル、インド、韓国、シンガポール、フィリピン、サウジアラビア、UAE、南アフリカ、エジプト、ナイジェリア等)、及び、6 国際組織・国際フォーラム（欧州評議会[CoE], 西アフリカ諸国経済共同体[ECOWAS]、欧州連合[EU]、サイバー専門知識に関するグローバルフォーラム[Global Forum for Cyber Expertise, GFCE]、国際刑事警察機構[INTERPOL]、米州機構[OAS]) の計 73 である。

2023 年 11 月 2 日に採択された「ランサムウェアへの支払に関する CRI 共同声明」においては、身代金の支払に関して次のような方針が示された。「我々（米国や日本を初めとする 46 か国及び INTERPOL）は、ランサムウェアのビジネスモデルを弱体化し犯罪活動を粉砕するためランサムウェアへの支払への我々のアプローチにつき集団で対処することを約束する。我々はしばしば無辜のふりをして行動するこれらのサイバー犯罪者の強要行為を許さない。従って、我々はあらゆる者がランサムウェアの要求のために支払をすることを強く思いとどまらせる。我々は各々模範を示すつもりである。我々は政府の権威の下にある関連機関がランサムウェアの要求に対しては、国内法令に従って、支払をすべきでないとの合意に達した。ランサムウェアの実行者への支払は、①事件の終了やウイルスに感染したソフトウェアのシステムからの除去を保証するものではなく、②犯人にこれらの活動を継続・拡大するインセンティブを与え、③犯罪実行者が不法な活動のために用いる資金を提供し、④データが戻ってくることを保証しない。我々は、INTERPOL を含む法執行を統合し、我々のレジリエンスを増大させ、これらの犯罪者が利用可能な資金を制限して、ランサムウェアによって我々の諸国に引き起こされた脅威に包括的に対処し続ける。」

諸政府のうちランサムウェアに対する身代金の支払に関する見解を最も明確に示しているのが米国政府である。身代金の支払は控えるべきというのが米国政府の基本的な立場で

あるが、特に 2021 年 9 月の米国財務省外国資産管理室（OFAC）の文書では、身代金の支払が違法になる場合があると警告する。英国の国家サイバーセキュリティセンター（NCSC）が 2024 年 5 月に示した文書でも「英国による制裁の対象となっている団体や地域に対する身代金の支払は違法になる」と指摘する。

ランサムウェアに対する身代金の支払を禁止する国内法令の稀有な例として、米国のノースカロライナ州法及びフロリダ州法がある。なお、ニューヨーク州には、ランサムウェアに対する身代金の支払を民間によるものも含めて禁止する法案が 2021 年に提出されているが成立には至っていない。

オックスフォード大学の Dapo Akande 教授をはじめとする国際法の専門家は、「サイバー空間における国際法上の保護に関するオックスフォード・ステートメント：ランサムウェア活動の規制」という文書を 2021 年に公表している。この文書の中で身代金の支払については、「国家は...可能な範囲で(to the extent possible) 身代金の支払を防止及び抑止することができる(may)」としている。身代金の支払を禁止する趣旨の must という単語が使われておらず、また、身代金の支払防止は「可能な範囲で」(to the extent possible) 行えばよいという両義的な表現ぶりとなっている。この文書は、国際人権・人道法に非常に注力しているが、半面、ランサムウェアが引きこした被害者の財産的価値の喪失への法的対応についての指摘がなされていない点が残念である。

留意すべきは、海賊とテロリズムという国際社会における代表的な国際犯罪は、身代金の支払の法的評価が大きく異なっているということである。海賊（「人類共通の敵」とされ、どの国家も刑事裁判権を行使できるという意味での普遍的管轄権が設定されている）については、海上保険の中心地であるため影響力が大きい英国の裁判所は、海賊への身代金の支払は英国法上、違法ではないとの判断を示している。これに対して、テロリズムについては、1987 年 6 月の G7 ヴェネチア・サミットにおける「テロリズムに関する声明」では、「テロリスト及びその支持者に対しいかなる譲歩も行わないとの原則に対するわれわれ各自のコミットメントを確認する」と謳っているように、テロリストとは取引しないというのが西側先進諸国の基本方針である。2009 年 12 月の国連安保理決議 1904 では、禁止されたテロリストへの資金供与は身代金の支払にも適用されると規定している。 2013 年 6 月の G8 ロック・アーン・サミットにおける「首脳コミュニケ」のパラグラフでは、「我々は，同決議に従い，テロリストに対する身代金の支払を全面的に拒否する」と謳っている。海賊とテロリズムの身代金の支払をめぐる評価の相違は、海賊の場合は経済犯罪（経済的利益を求めての犯罪）であって、身代金を支払えば通常は船員は釈放され船体は返還されてきたのに対して、テロリズムの場合には政治犯罪（政治的な動機・目的に基づく犯罪であって、身代金の要求があっても通常それは政治的な要求に付随してなされるに過ぎない）であり、身代金を支払うことだけで人質が釈放されることは通常は期待できないといった相違に基づくものであると考えられる。

ランサムウェア攻撃は海賊とテロリズムのいずれに類似しているのであろうか。ランサムウェア攻撃は経済犯罪という側面が強いという点では海賊に近いが、身代金の支払により復号化によるデータの復旧の見込みがどこまで期待できるか未知数であるという点ではテロリズムに近く、いずれに近いとも言い難いのが実情である。

ランサムウェアの要求に対する身代金の支払を非難することは、その放置が一層の身代金の要求につながりかねないことに鑑みると一般予防の観点から非常に重要である。この点から、国際カウンターランサムウェア・イニシアティブにおいて「ランサムウェアの要

求に対しては支払をすべきでない」旨の合意をしたことは、ポジティブに評価されるべきであり、「サイバー空間における法の支配」の確立に資するものである。但し、例外的に身代金の支払を非難しない方が良い場合も存在し得ることに留意しなければならない。例えば、コロニアル・パイプライン社へのランサムウェア攻撃においては、同社はデータの復旧がなされないとエネルギー供給に多大の支障・混乱が生じて米国のエネルギー安全保障を大きく損なうと判断して身代金を支払った。米国政府は同社のこのような行動を強く非難しなかったが、国際カウンターランサムウェア・イニシアティブにおいて、「我々はあらゆる者がランサムウェアの要求のために支払をすることを強く思いとどまらせる。我々は各々模範を示すつもりである。」と述べていることとどう整合するのであろうか。

たとえ身代金の支払を禁止する一般的なルールが確立されているとしても、緊急避難（国家責任条文第 25 条）に該当する場合には支払が容認されうることになる。具体的には、政府機関の最重要データや重要インフラのデータがランサムウェア攻撃を受け、身代金支払の要求に応じずデータが復旧されないままだと、「重大かつ差し迫った危険を守る」ことができなくなってしまうという場合が考えられる。このような場合には、最悪の事態を回避するために例外的に身代金支払の要求に応じたり、応じた企業・団体の行動を黙認したりすることはやむを得ないと考えられる。

ランサムウェアに対する身代金支払は保険でカバーされるか。サイバー攻撃に対処するための保険としてサイバー保険があるが、日本の保険会社はランサムウェアに対する身代金支払は補償対象外としている。外国の保険会社の対応は様々なようである。米国政府のサイバー・新興テクノロジー担当国家安全保障副補佐官の Anne Neuberger は、「ランサムウェアの支払の求償をカバーするようないくつかの保険会社の政策は身代金の支払にインセンティブを与え、サイバー犯罪のエコシステムを焚きつける。これは問題のある慣行であり、終了しなければならない」と指摘している。

サイバー保険に関しては、英国王立防衛安全保障研究所（RUSI）の報告書では、ランサムウェアを誘発するという批判の一方で、身代金支払の成長を安定化させ、被害者が内容を知らされた上で決定することを可能にし、法外な要求の支払をしてしまうことでより多くの犯罪者がこのエコシステムに加わろうとする意欲を削ぐことが可能となるとする。つまり、「身代金の規律」がサイバー保険によってなされるとする。

ランサムウェアの要求に従って支払った身代金は損金として税控除の対象になるか否かは興味深い主題である。一般論として、①身代金の支払が違法であれば税控除の対象にはならない、②たとえ違法でなくても、身代金支払を控えるようにと政府が呼びかけている以上、税控除を認めてしまうとその呼びかけとの矛盾が生じるため認めるべきではない、と考えるのが合理的であろう。

ランサムウェア攻撃による身代金の支払手段として主として暗号通貨による支払が要求されること、及び、コロニアル・パイプライン事件において米国政府がその一部を奪還したことについて。暗号通貨が身代金の主要な支払手段になったことは、ソマリア海賊の身代金については空から 100 ドル札で海賊船に落下させるという原始的な方式で支払われたこととは対照的である。コロニアル・パイプライン事件における米国政府による身代金の一部は新設のランソムウェア及びデジタル強奪タスク・フォースによって実施された。FBI が身代金を得たビットコイン口座の暗号キーを入手し、口座に入りこんで奪還したとされる。

8. エストニアとモナコのサイバー大使館

日本では想像もつかないことだが、エストニアとモナコは国家の最重要データのバックアップを国外におくという選択をしている。

エストニアは2007年にロシアからサイバー攻撃を受け、一時は国家機能が麻痺するほどの損害を受けた。この経験や2014年のロシアによるクリミア併合から、エストニアは、バックアップの電子データを国外に保管することが国家運営の継続性を確保するために不可欠であると判断してその検討をすすめた。エストニアは電子化が高度に進んだため、紙でのバックアップ・データの保管はおよそ現実的ではなく、バックアップ用の電子データを国外で保管することで digital continuity を確保することが必要だと判断した。また、既存のエストニア大使館をデータのバックアップ用に利用することは、エストニアや接受国における危機の際には不十分であってデータ・センターでの保管が必要だと判断した。その上で、エストニアは、①友好国に所在する自国の大使館にデータを保管するオプションと②民間のクラウド・サービスを利用してデータを保管するオプションを検討したが、データに対して完全なコントロールと管轄権を保持する必要上、②のオプションでは不十分だと判断して、①のオプションを採用することとした。

エストニアはデータ大使館（data embassy）を政治的に最も安定した富裕国であるルクセンブルクに設置することに決定し、2016年11月14日の両国間の了解覚書（MoU）を経て、2017年6月20日に両国間でデータ及び情報システムのホスティングに関する協定が締結された（2018年には両国の議会において同協定の批准が承認された）。そして2018年にはルクセンブルク東部の Berzdorf にデータ大使館が設置された（5年間のレンタルで代金は220万ユーロだとされる）。

データ大使館は通常の大使館では勿論ないが、一定の不可侵権を有する。「捜索、徴発、差押え及び強制執行からの免除」については大使館並みの免除が付与されている。他方、データ大使館への立ち入り可否の基準については領事館並みであるといえる（火災の場合には同意があったものとみなして中に入れる）。保管対象となるデータの国際法上の地位とデータに対する保護水準については、「装置及びライセンスは、エストニアの資産とみなされ、いかなる形態の法的手続からも免除される」旨、規定する。また、データ大使館内にあるデータ及び情報システムはエストニアの公文書とみなされるとした上で、データ及び情報システムは「不可侵であり、捜索、徴発、差押え及び強制執行を免除される」と規定する。

さらに、エストニアのデータ大使館に対するサイバー攻撃の場合には、ルクセンブルクは大使館に付与するのと同じ優先的待遇をデータ大使館に付与するという趣旨の規定もおかれている。

モナコもほぼ同様のサイバー大使館協定をルクセンブルクとの間で2021年に締結した。エストニアがロシアに脅威に常にさらされているのとは対照的にモナコにとって脅威国はないが、万が一の場合に備えていることが注目される。なお、データ大使館を提供する用意のあるのはルクセンブルクだけではない。バーレーンは2018年にデータ大使館を提供する法体制を整えている。もっとも中東という地政学的リスクの高い地域ゆえに「客」がくるのか、限界があるのではないかと思われる。

9. 経済安全保障とサイバー

経済安全保障（economic security）の確立された定義はないが、①経済的な力を安全保障目的や外交目的のために利用すること(economic statecraft)、②重要インフラの保護や不可欠な資源・食糧の確保などのために諸措置をとること、③自由で開かれた国際経済秩序を維持・強化すること、を主な内容とすると考えられる。

①は、economic statecraft とも言われ、経済制裁（economic sanctions)がその代表例である。②は、エネルギー安全保障や食糧安全保障がその代表例である。2022 年に施行された経済安全保障推進法も、ここに属する。同法では、A. 特定重要物資の安定的な供給の確保、B. 特定社会基盤役務の安定的な提供の確保、C. 先端重要技術の開発支援、D.特許出願の非公開という 4 つの施策を内容とするものである。A につき、半導体、重要鉱物、天然ガス、永久磁石、航空機部品、蓄電池など 11 の特定重要物資を指定して、事業者の計画認定や支援措置を定め、政府による備蓄措置などを規定する。B につき、基幹インフラとして、電気、ガス、石油、水道、鉄道、航空、空港、電気通信、放送、郵便、金融、クレジットカードなどの 14 分野を定め、重要施設の導入や維持管理の委託の事前審査や勧告・命令について規定する。C につき、海洋、航空・宇宙、サイバー・ AI、バイオの領域での 27 の先端重要技術を定め、資金支援や調査研究の委託につき規定する。D につき、G20 のうち非公開特許制度を採用していないのは日本、アルゼンチン、メキシコのみであった（日本は戦前には非公開特許制度を採用していた）が、安全保障上機微な発明の特許出願について公開・流出を防止し、他方、発明者には対価を補償する。同法 90 条においては、「この法律の施行に当たっては、我が国が締結した条約その他の国際約束の誠実な履行を妨げることがないよう留意しなければならない」として、国際約束の誠実な履行をうたっており、特に国際法違反の問題が生じる可能性を心配する必要はない。同法は主に先端技術安全保障を対象にするものといえる。それ自体の重要性はいうまでもないが、古典的な経済安全保障であるエネルギー安全保障及び食料安全保障の重要性も不変であり、ロシアのウクライナ侵略はこれらの脆弱性を再認識させたともいえる。

経済安全保障が現代国際社会において重要性を増しているのは、第 1 に、中国・ロシア・北朝鮮対西側諸国の対立に代表されるように、国家間の地政学的リスクが高まっていること、第 2 に、冷戦後の約 30 年間において経済的な相互依存関係が深化したことや、IT 化の進展に代表されるように経済の影響力が増大したことがその主な要因であると考えられる。

国際法は国際社会の共通言語（*lingua franca)* であり、国家ができること（許容）、やらなければならないこと（義務）、やってはいけないこと（禁止）を示すものでもあり、法治国家における外交政策の基本指針を示すものだといえる。

サイバーに特化して経済安全保障との関係を考えてみると、①についてはサイバー力を安全保障目的や外交目的のために利用することである。これはサイバー攻撃やサイバ―諜報に限られず、サイバー分野での信頼醸成措置や能力構築によりサイバー外交を展開することが該当すると考えられる。日本のサイバー外交の場合、サイバー対話を通じて各国との協力関係をすすすめているが、米国とは同盟国としてサイバー空間でも同盟関係を強化する、EU 諸国とは価値観を同じくする友好国としてサイバー分野でも最先端の協力を推進する、ASEAN 諸国にはサイバー分野での能力構築（capacity building)を行う、中国やロシアに対しては信頼醸成措置（CBM）を推進するといった見取図があると考えられる。米露間や米中間で合意されたサイバー攻撃やサイバー諜報に関する CBM が日中間でも合意されても良いと考える。②に関しては、「C. 先端重要技術の開発支援」の中にサイバー分野での

以下の技術も支援対象に含まれている。AI セキュリティに係る知識・技術体系、不正機能検証技術（ファームウェア・ソフトウェア／ハードウェア)、ハイブリッドクラウド利用基盤技術･先進的サイバー防御機能・分析能力の強化 、サイバー空間の状況把握・防御技術、セキュアなデータ流通を支える暗号関連技術、偽情報分析に係る技術、ノウハウの効果的な伝承につながる人作業伝達等の研究デジタル基盤技術。③に関しては、サイバー分野では経済サイバー諜報が TRIPS 協定に違反する可能性が高いことが関連する。