能動的サイバー防御の国際法枠組み
武力未満と違法性阻却による正当化の可能性

黒﨑 将広
Kurosaki Masahiro

［要旨］
「能動的サイバー防御」（ACD: Active Cyber Defense）を規律する国際法枠組みで中心となるのは、武力行使禁止原則、不干渉原則および主権原則である。しかし、今後ACDとして実施されるサイバー行動がいかなる場合にこれら諸原則の違反となり得るかは、個別具体的な状況次第であることはもちろん、各国の見解もさまざまであるため、予断を許さないのが現状である。
それだけに、日本がACDの合法性を担保するうえで違法性阻却事由は重要な位置を占めることとなる。この点については対抗措置または緊急避難が選択肢として考えられるが、これらの事由が武力行使の違法性までを阻却することができないことには注意が必要である。しかもACDが武力攻撃に至らないサイバー攻撃のおそれの段階で実施される限り、武力攻撃の発生を条件とする自衛権でこれを正当化することもできない。このことからACDを実施するにあたっては、国際法上禁止される武力に至らないようサイバー行動を抑制することが求められる。

はじめに

2022年12月に発出された国家安全保障戦略で、日本政府は「能動的サイバー防御」（以下、「ACD」）と呼ばれる新たなサイバー安全保障戦略の導入を打ち出した。これは「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」しようとするものである(1)。これまで日本のサイバー安全保障については、2018年12月の防衛大綱で打ち出された「有事において、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力」（傍点筆者）(2)に焦点があてられていたが(3)、日本の防衛機密ネットワークへの平素からの侵入がいっそう懸念される中で(4)、今後は、平時の段階でこれを未然に防ぐサイバー対処行動にも焦点をあてることで、防衛能力の強化を試みようとするものであると言える。
とはいえ、現在は「能動的サイバー防御の実施のための体制を整備」(5)する段階にあるうえ、サイバー安全保障がそもそも機密性の高い分野でもあることから、具体的にどのような対処行動が現在想定され、またその全体像が今後どこまで明らかになるかは定かでない。

ACDを実施するのは誰なのか――例えば自衛隊がこれを行うのか――、それとも「内閣サイバーセキュリティセンター（NISC）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織」[6]が直接これを行うのかも不明である。他方、「可能な限り未然に攻撃者のサーバ等への侵入・無害化ができる」[7]と明示されている点は注目に値する。

以上のことから推察されるACDとは、少なくとも次のような行動を想定するものと言えるだろう。すなわち、①武力攻撃に至らない日本の「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（possibility）がある場合」に実行する、②（情報収集および分析を通じて）攻撃を行うおそれのある者および使用されるサーバその他攻撃手段、ならびにそれらの位置等を特定する、③サイバー手段（情報通信技術）を用いて対象を「排除（eliminate）」または「無害化（neutralize）」する、そして④これらのために必要に応じてコンピュータおよびインターネットその他のネットワークまたはシステムに（おそらくは日本から遠隔操作で）「侵入（penetrate）」する、ということである。このうち国際法上、特に問題となるのは、③と④により他国に物理的または非物理的な損害その他の影響（データ改ざんを含む）が生じる場合だろう。

こうしたサイバー行動（cyber operations）を国外の対象に向けて実施する際、日本はいかなる国際法上の規律に服するのだろうか。本稿では、今後日本がACD実施のための態勢整備を進めていく際の基本的留意事項を提示すべく、適用可能な主たる一般国際法の枠組みに即してこの問題を整理し検討することとしたい[8]。

1　禁止規範

（1）　武力行使禁止原則

ACDの国際法枠組みを考えるうえで何よりもまず注意しておかねばならないのは、それが武力行使禁止原則に抵触する可能性である。ACDが武力攻撃に至らない重大なサイバー攻撃のおそれに対するものである以上、武力攻撃の発生を要件とする国際法上の自衛権（国連憲章51条）にこれを基礎付けることはできない。したがって、ACDとして実施される外国コンピュータネットワークへの侵入および対象の排除または無害化が武力行使となれば、当該外国の同意または国連安全保障理事会の許可がない限り国連憲章2条4項違反となってしまう。

もっとも、サイバー行動は一般的に物理的被害を引き起こすことがまれであると考えられているため、ACDもまた「本質的には国連憲章2条4項における武力には該当しない」[9]との主張がなされるかもしれない。しかし日本政府自身が「サイバー行動であっても、一定の場合には、国連憲章第2条4項が禁ずる武力による威嚇又は武力の行使に当たり得る」と認めるように[10]、少なくとも次の理由からACDが武力行使禁止原則違反となる可能性は完全に排除できないように思われる。

第1の理由は、現時点で国際法上確立した武力行使の定義が存在しないからである。しかも、禁止される武力の下限（*de minimis* threshold）をめぐる解釈も国家間で必ずしも一致していない。例えば、2018年3月4日に英国のソールズベリーで起きたロシアによる元諜報員殺人未遂事件で英国が当該行為を自国に対する「違法な武力の行使であり国連憲章2条違反」

と非難したように[11]、低烈度のサイバー行動であっても国によっては武力行使禁止原則違反と判断するかもしれない[12]。

第2の理由は、たとえACDの一環として実施される日本のサイバー行動が単独では武力行使を構成しなくても、同国によるほかの行動と集積させることで総合的に武力行使の敷居に達する余地が国際法上残されているからである。「集積理論（accumulation of events theory）」と呼ばれるこの解釈アプローチは、国際司法裁判所（ICJ）が、個別的にみれば武力行使に至らない一連の行為を集積させることで武力攻撃と評価する可能性を否定しなかったことに着目するものである[13]。同裁判所が「規模と効果（scale and effects）」を基準に武力攻撃を「武力の行使の最も重大な形態（the most grave forms of the use of force）」と定義していることにかんがみ[14]、近年では「武力攻撃」だけでなく「武力の行使」自体の評価についても集積理論が適用可能であるとして、サイバー行動を武力の問題と捉えるべきとする見解もみられるようになっている[15]。

(2) 不干渉原則および主権原則

また、ACDの実施がたとえ武力行使を構成しなくても、その対象が位置する外国への干渉または主権侵害を構成すれば国際法違反となる[16]。

国際法上、ある国の行為が禁止される他国への干渉となるには、国籍、関税、出入国管理その他政治・経済・社会・文化に関する体制選択および外交政策形成といった国内管轄事項、すなわち「国家主権の原則によって各国が自由に決定することのできる事項」[17]に対して「威圧（coercion）」が働いていることが求められる。サイバーの文脈では、例えばある国の選挙実施の阻止もしくは選挙結果の改ざんのために選挙システムを操る外国のサイバー行動、またはある国の議会の基本的業務もしくは金融システムの安定に介入する外国のサイバー行動がその国の国内管轄事項に対する違法な干渉になり得るとの見解がこれまで示されてきた[18]。

他方、国内管轄事項に対するいかなる行為が威圧となるのかについては、確立した国際法上の定義や概念的境界が存在しない。実際、各国の見解はさまざまであり、近年ではサイバー手段による干渉の文脈で威圧を「そうでなければ自発的に追求することがないような行動方針（作為または不作為を問わない）をとるよう国家に強いる」[19]行為や、国内管轄事項を「管理し、決定しまたは規律する能力（the ability to control, decide upon or govern）を他国から効果的に奪う、または奪うことを企図した」[20]行為であると解する見解等が示されている。英国は、威圧を国内管轄事項に対する国家の「管理の自由（freedom of control）」を奪う行為であるとの見解を示すなど、サイバーの文脈で禁止される干渉の範囲を広く捉えているようにも見受けられる[21]。このような立場をとる国が存在することにかんがみれば、場合によっては日本のACDによって自国のサイバー安全保障政策の変更を余儀なくさせられたとして、対象の所在する領域国が日本のサイバー行為を違法な干渉と非難するかもしれない。

さらにたとえ干渉行為を構成しなくても、ACDが対象国の領域主権の侵害となる可能性は残されている[22]。主権原則は、国家領域を基礎とする国際法秩序のいわば最後の砦とも言うべき「最も重大な、超えてはならない一線」[23]として、国家によるサイバー行動を規律する。問題はいかなる場合に主権侵害が発生するのかであるが、専門家の間では、ある国の領

域に物理的損害を引き起こすか、あるいは本質的な政府機能に対する介入（interference）または同機能の剥奪を引き起こす場合がそうであるとされる[24]。しかし、各国がこれを支持しているかどうかは必ずしも定かではない。事実、自国のネットワークに影響をもたらすすべての外国のサイバー行動は主権侵害になり得ることを示唆するフランスから、そもそもサイバー行動によって干渉とは独立して主権侵害が発生することはないと考える英国[25]に至るまで、見解はさまざまである[26]。日本は「医療機関を含む重要インフラに対するサイバー行動によって物理的被害や機能喪失を生じさせる行為」が主権侵害を構成し得るとの立場を示しているが、こうした各国の立場の違いは、サイバー空間を自国領域（領土一体性）の問題としてどこまで位置付けるのか、また、何を自国の本質的な政府機能の問題と位置付けるかについての捉え方の違いを反映しているとみることができる[27]。

このように、自国に向けて行われる外国の越境サイバー行動が違法な干渉あるいは主権侵害となる可能性が高いことを主張することで他国を牽制しようとする立場が国によっては強く見受けられる現状を踏まえると、日本がそうした国に所在する対象に向けてACDを実施する限り、常に国際法違反と非難されるリスクが付きまとうこととなる。それだけにACDの国際法枠組みを考えるにあたっては、違法性阻却事由に基づく正当化の選択肢を常に考慮に入れておく必要があると言えるだろう。この場合、適用可能な事由は、①対象所在国の同意、②対抗措置、および③緊急避難が基本的に考えられるが（国家責任条文20、22、25条）、当該国がACDの違法性阻却に同意しない限り、日本は対抗措置または緊急避難を援用するよりほかはない。ただし、対抗措置と緊急避難は武力行使の違法性まで阻却しないため――武力行使はあくまでも自衛、国連安保理の許可または相手国による同意の場合にのみ許される[28]――、以下では不干渉原則と主権原則の違法性阻却が可能か否かを検討することとする。

2　違法性阻却事由

（1）　対抗措置

ACDの対象国が日本に対して国際法違反を先行して行っている場合、それを止めさせる自力救済のための対抗措置（countermeasures）として日本はACDの違法性阻却を主張することができる――ただし、当該措置は第三国に対する違法性までを阻却するものではない[29]――。この自力救済の権利は、相手国が違反した「義務の遵守を促すためにのみ」認められるため、ACDの文脈では、①対象が国であること、および②その国が先行違法行為を行っており、かつその違法行為により日本が被った被害と均衡するものでなければならないといった制約がある（国家責任条文49～54条）[30]。

①の制約については、とりわけACDの対象が非国家行為体である場合に深刻な問題となるだろう。そこには、日本政府も認めるように「サイバー行動の特徴の一つとして、国家への帰属の判断が困難」であるという現状があるからである[31]。したがってこの場合は、当該帰属を立証するよりもむしろ、「同行動の発信源となる領域国」が自国「領域を他国の権利に反する行為にそれと知りつつ使わせてはならない」[32]相当の注意義務（領域使用管理責任）に違反していることを理由に、当該領域国に対する対抗措置としてACDを正当化するのが得策

であるかもしれない。実際、日本は、サイバー行動に適用可能な相当の注意義務の一つとして、「他国の重要インフラを害するといった重大で有害な結果をもたらすサイバー行動」に関与する者が自国領域内にいるという「信頼に足る情報を他国から知らされた」国は当該行動を行わないようその者に「影響力を行使する義務」があるとの見解を示している(33)。ただし、他方で相当の注意義務自体が一般的義務としてサイバー空間に適用されることに否定的な国も一部には存在することには注意を要する(34)。

②については、日本のACDが自国へのサイバー攻撃を未然に防ぐことを目的としている以上、当該攻撃のおそれがあるというだけで相手国にいかなる先行違法行為が存在すると言えるのかが問題となる。これは、上述の相当の注意義務の射程が私人のサイバー行動に対する領域国の予防にまで及ぶのかどうかにもかかわってくる(35)。また、日本政府は「一般国際法上、対抗措置が先行する国際違法行為と同様の手段に限定されなければならないとの制約はなく、このことは、サイバー空間における国際違法行為に対する対抗措置についても同様だと考えられる」との見解を示しており(36)、ACDについてもその時の具体的な状況に応じて先行違法行為の存在をサイバーの文脈に限らず広く対象所在国に見出すことができるかもしれない。

(2) 緊急避難

これに対して、もう一つの違法性阻却事由である緊急避難の抗弁（the plea of necessity）は、以上のような対抗措置が抱える問題のいくつかを克服することができる点で、日本のACDに最も適した国際法枠組みと言えるかもしれない。そこでは誰が責任を負うかではなく危険回避に何が必要かという点が重視されるため(37)、相手国の先行違法行為も国家への行為帰属も求められず(38)、しかも第三国に対する行為の違法性をも阻却できる「唯一の選択肢」(39)を提供し得るものとされているからである(40)。これは、「デジタルインフラが有する高度の相互接続性と相互依存性ゆえに第三国への意図せぬ損害が発生することが考えられる」(41) ACDにとっては極めて重要な利点である。

しかしそれだけに緊急避難の抗弁には濫用の危険性が常に伴うため、国際法上の違法性阻却事由としてこれを認めることに多くの批判が集まってきたのも事実である(42)。これを踏まえて国家責任条文では、「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」である場合に緊急避難の抗弁が認められ得る等の制限が設けられた（25条）(43)。日本政府はサイバー行動への適用についても「国家責任条文25条に示された要件に合致する場合には緊急避難を援用することも国際法上認められている」(44)との立場を明確にし、当該抗弁の実定法性を認めている。

緊急避難の諸要件のうち「根本的利益」とは、国際共同体全体の利益も含まれ得るが、基本的には国家の利益を指す。このことから、サイバー攻撃の文脈では「銀行システム、証券取引所、航空機の離発着、鉄道輸送、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ざん、環境損害の発生、配電網の遮断、国の食糧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」と解されている(45)。

緊急避難については、サイバー攻撃のおそれがある段階での先制的な、または未然の対処をACDとして正当化することが可能である点も重要であろう。ただ、それだけに根本的利益に対する危険性の重大性と急迫性の存在は客観的に立証されねばならず――とりわけ「危険が差し迫っていると言うためには、それを回避する『最後の好機（last window of opportunity）』」であることが必要とされる[46]――、また講じられる措置も唯一の方法でなければならないため、他国や国際組織からの協力が得られる等のほかの選択肢がある場合、ACDの正当化に緊急避難を援用することはできない[47]。このように緊急避難は極めてまれな場合に援用可能な例外事由である以上[48]、緊急時の一時的な抗弁でしか認められないという限界がある。ゆえに緊急避難はACDを正当化する「初期設定（default）」[49]の枠組みとして適さないことはもちろん、とりわけ米国のような武力紛争に至らない範囲で「先行防御（defending forward）」を「常時実施（persistently engage）」するサイバー行動の場合には、個別行動毎にいっそう慎重さが求められる正当化の枠組みであると言えよう[50]。

おわりに

ACDを規律する国際法枠組みで中心となるのは、武力行使禁止原則、不干渉原則および主権原則である。しかし、今後ACDとして実施されるサイバー行動がいかなる場合にこれら諸原則の違反となり得るかは、個別具体的な状況次第であることはもちろん、これまでの検討で明らかにしたように国によって見解がさまざまであるため、予断を許さないのが現状である。そこには、これら諸原則を通じて外国のサイバー行動から自国の何を保護しようとするのかという安全保障上の保護法益をめぐる各国の考え方の違いが背景にある。これを政策に活かすなら、日本はACDの対象とする国とそれにより影響を被る可能性のある国が以上の国際法原則についていかなる立場を有しているのか――あるいは立場を明らかにしていないのか――を安全保障環境の変化に合わせて絶えず精査しつつ、これら諸原則の違反が各方面から主張されるリスクを個別事案に即して想定しておく必要があるだろう。

それだけに、日本がACDの合法性を担保するうえで違法性阻却事由が重要な位置を占めることは言うまでもない。しかしながら対抗措置は、先行違法行為と当該行為の国家への帰属の証明を要するうえ、第三国に引き起こした違法性までをも阻却しない点でACDを正当化する際には大きな障害となることが予想される。他方、緊急避難はこうした問題を引き起こさない点でACDに最も適した違法性阻却事由とみることができるかもしれないが、濫用の危険性も含めてさまざまな論争を呼んできた一般国際法規則でもある。それゆえ、サイバー安全保障分野において「国際的な枠組み・ルールの形成等のために引き続き取り組む」うえで緊急避難を検討する際には[51]、サイバー空間の独自性を考慮しそれに特化した制度として同規則を発展させていくべきかもしれない。

ただし、対抗措置と緊急避難のいずれも武力行使の違法性までを阻却するものではない。ACDが武力攻撃に至らないサイバー攻撃のおそれの段階で実施される限り、武力攻撃の発生を条件とする自衛権でこれを正当化することはできないことから、国際法上禁止される武力に至らないようサイバー行動を抑制しなければならないことも忘れてはならない。

（1）「国家安全保障戦略について」令和4年12月16日（国家安全保障会議決定・閣議決定）、21ページ。

（2）「平成31年度以降に係る防衛計画の大綱について」平成30年12月18日（国家安全保障会議決定・閣議決定）、18、24ページ。

（3） この点については、Masahiro Kurosaki, "The Projection of Cyber Power by Australia and Japan: Contrasting Their Doctrines and Capabilities for the Rule-Based International Order," The United Nations Institute for Disarmament Affairs（UNIDIR）(ed.), *International Cyber Operations: National Doctrines and Capabilities*（UNIDIR, 2021）, pp. 6–9を参照。

（4） 実際、2020年秋に中国人民解放軍が日本の防衛機密ネットワークに侵入したとの通報が米国から日本政府になされたとの報道がある。*See* Ellen Nakashima, "China hacked Japan's sensitive defense networks, officials say," *The Washington Post*, August 8, 2023. もっとも、これに対して日本政府は「サイバー攻撃により、防衛省が保有する秘密情報が漏洩したとの事実は確認しておりません」との見解を示している。防衛大臣記者会見、令和5年8月8日。

（5）「国家安全保障戦略について」、21ページ。

（6）「国家安全保障戦略について」、22ページ。

（7） 同上。

（8） したがって、本稿で扱わない個別条約その他国際法規則の適用可能性は今後の検討課題に委ねられる。

（9） Johann-Christoph Woltag, "Cyber Warfare," Max Planck Encyclopedias of Public International Law, August 2015, para. 3.

（10） 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」2021年5月28日、6ページ。日本政府によれば、「武力による威嚇とは、一般に、現実にはまだ武力を行使しないが、自国の主張、要求を入れなければ武力を行使するとの意思、態度を示すことにより、相手国を威嚇することをいう」。

（11） UN Doc. S/PV.8203, March 14, 2018, p. 2. *See also* Prime Minister's Office, 10 Downing Street and The Rt Hon Theresa May MP, "A statement to the House of Commons by Prime Minister Theresa May following the Salisbury incident," Gov. UK, March 14, 2018.

（12） この点については、黒﨑将広「自衛隊による『武器の使用』は『武力の行使』とは違う？――国際法上禁止される『武力の行使』と憲法の制約」森川幸一ほか（編）『国際法で世界がわかる――ニュースを読み解く32講』（岩波書店、2016年）も参照。

（13） *See Oil Platforms*（*Islamic Republic of Iran v. United States of America*）*, Judgment, I.C.J. Reports 2003*, para. 64. *See also Military and Paramilitary Activities in and against Nicaragua*（*Nicaragua v. United States of America*）*, Merits, Judgment, I.C.J. Reports 1986*（*The Nicaragua Judgment*）, para. 231.

（14） *See, e.g.*, *The Nicaragua Judgment*, paras. 191, 195.

（15） *See, e.g.*, Michael McLaughlin, "Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace," *Opinio Juris*, March 2, 2023. 中谷和弘ほか『サイバー攻撃の国際法――タリン・マニュアル2.0の解説（増補版）』（信山社、2023年）、85～86ページも参照。

（16） 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」2ページ。保険医療・公衆衛生分野における当該国際法規則のサイバー行動への適用を扱った研究として、黒﨑将広「サイバー空間における保健医療・公衆衛生分野の保護と国際法規範――デジタル情報通信技術の空間性と領域性原理の機能的再定式化」『国際法外交雑誌』第120巻1・2号合併号（2021年）も参照。

（17） *The Nicaragua Judgment*, para. 205. 友好関係原則宣言第3原則「いかなる国又は国の集団も、理由のいかんを問わず、直接又は間接に、他国の国内又は対外の事項に干渉する権利を有しない」。

（18） *See, e.g.*, Attorney General's Office and the Rt Hon Sir Jeremy Wright KC MP, "Cyber and International Law in

the 21st Century," Gov. UK, May 23, 2018; Australian Government, "Australia's Submission on International Law to be Annexed to the Report of the 2021 Group of Governmental Experts on Cyber," June 2021, p. 3.

(19) The Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace – Appendix: International law in cyberspace, September 26, 2019, p. 3.

(20) Australian Government, *supra* note 18, p. 3.

(21) *See, e.g.*, Attorney General's Office and The Rt Hon Suella Braverman KC MP, "International Law in Future Frontiers," Gov. UK, May 19, 2022.

(22) 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」、3ページ：「日本政府としては、不干渉原則により禁じられる違法な干渉とは必ずしも一致しない主権侵害が存在すると考えてきている」。

(23) Michael N. Schmitt and Liis Vihul, "Sovereignty in Cyberspace: *Lex Lata Vel Non?*" *AJIL Unbound*, Vol. 111 (2017), p. 213.

(24) *See, e.g.*, Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), pp. 20–23.

(25) もっとも英国は、サイバー空間における主権侵害の可能性を否定する代わりに、上述のように武力行使禁止原則と不干渉原則の下限を低く設定することで外国による自国へのサイバー行動を牽制しようとしているのかもしれない。

(26) こうした英仏を含む国家実行の状況を整理した研究として、御巫智洋「インターネットの利用に関する国際的なルールにおいて領域主権が果たす機能」『国際法外交雑誌』第121巻第1号（2022年）を参照。

(27) この点については、外国への越境サイバー行動を積極的に「する側」と「される側」の視点も重要になるだろう。黒﨑将広「サイバー空間における主権――その論争が意味するもの」森肇志・岩月直樹（編）『サブテクスト国際法』（日本評論社、2020年）を参照。

(28) ただし、タリン・マニュアルの専門家集団の中では緊急避難の場合に武力行使が許容されるかにつき見解の一致がみられなかったという。中谷ほか、前掲書（注15）、38ページ。

(29) UN International Law Commission (ILC), Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, 2001, pp. 75–76, paras. 1, 5 (Art. 22).

(30) なお、対抗措置の条件として国家責任条文52条1項(b)では対象国への事前通告が規定されているが、これを義務的な国際法規則として秘匿性の高いサイバー行動に適用することについては否定的な見解が根強い。*See, e.g.*, Attorney General's Office and the Rt Hon Sir Jeremy Wright KC MP, *supra* note 18.

(31) 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」、5ページ。

(32) 同上。

(33) 同上。この点については、コロニアル・パイプライン社へのサイバー攻撃実行者がロシアに所在するとの通報を米国がロシアに行った事案が参考になる。*See* White House, Remarks by President Biden on the Colonial Pipeline Incident, May 13, 2021.

(34) 御巫、前掲論文（注26）、16～23ページ。

(35) この点について詳しくは、Talita Dias and Antonio Coco, *Cyber Due Diligence in International Law* (Oxford Institute for Ethics, Law and Armed Conflict, 2021) を参照。

(36) 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」、4ページ。中谷ほか、前掲書（注15）、35ページも参照。

(37) *See, e.g.*, Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge University Press, 2020), pp. 201, 255–256.

(38) ILC, *supra* note 29, p. 80, paras. 2 (Art. 25).

（39） Schmitt（ed.）, *supra* note 24, p. 138, para. 10.

（40） ただし、第三国の不可欠の利益を著しく害する場合は緊急避難でも違法性阻却が認められないとされている。*See ibid*., p. 137, paras. 6–8.

（41） Christian Schaller, “Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual’s Conception of Necessity,” *Texas Law Review*, Vol. 95（7）（June 2017）, p. 1620.

（42） この点も含め、国家責任条文が定式化した緊急避難の抗弁の実定法的性格に疑義を呈するのみならず、それが国家実行や裁判例において支持されてきた従来の「緊急避難」に基づくものでもないことを論証する近年の研究として、北村朋史「国際法上の緊急避難に関する一考察――二つの「緊急避難」と国家責任条文二五条の意味（上）～（下・二）」『法学会雑誌』55巻2号・56巻1・2号（2015～16年）を参照。

（43） ILC, *supra* note 29, p. 83, paras. 13–14（Art. 25）.

（44） 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」、4ページ。

（45） 中谷ほか、前掲書（注15）、37ページ。

（46） 同上。

（47） ILC, *supra* note 29, p. 83, paras. 15（Art. 25）. 中谷ほか、前掲書（注15）、38ページ。

（48） ILC, *supra* note 29, p. 80, paras. 1–2（Art. 25）.

（49） Lahmann, *supra* note 37, p. 257.

（50） U.S. Department of Defense, 2023 Cyber Strategy: Summary, September 12, 2023.

（51） 「国家安全保障戦略について」、22ページ。

くろさき・まさひろ　防衛大学校教授