第　〇　章

サイバー攻撃に対する国際法の適用

東京大学大学院教授
西　村　　弓

Ⅰ　はじめに

情報通信技術（Information and Communications Technologies：ICT）の発達と当該技術に対する社会規模での依存度が高まることに応じて，サイバー攻撃（何らかの意図や悪意を持った者が，特定の国家や企業，団体，個人に対して，コンピュータ・ネットワーク上で行うクラッキング行為）が社会基盤を脅かし得る重大な脅威となりつつある。こうした事態に対応して，国内外でサイバーセキュリティの強化が急務となっている。エネルギー産業分野においても，G7エネルギー大臣ハンブルク会合（2015年）が「持続可能なエネルギー安全保障のためのG7ハンブルク・イニシアティブ」を公表して，「エネルギー輸送システムへのサイバー上の脅威はますます複合的で巧妙になってきている。我々の経済は，インフラやサービスをモニターし管理する相互に接続されたICT設備を通じて，エネルギーの産出，輸送および分配を確保するデジタルネットワーク上のシステムを基盤として成り立っている。エネルギーのバリューチェーン全体を通じてこれらのシステムが運用され相互接続される必要性は日々増大しており，そのためにデジタル上のフレームワークおよびインフラを維持する必要性も増している」という当時の現状認識を示すとともに[1]，「我々は，エネルギー分野におけるサイバーセキュリティの改善に向けて取り組むことを約束する。そうした取り組みには，異なるアプローチの分析，サイバー上の脅威の識別，脆弱性およびベストプラクティスの定義や方法に関する情報交換，サイバーセキュリティ能力向上への投資や能力構築が含まれる」としてエネルギー分野におけるサイバーセキュリティ向上の必要性を謳っている[2]。とりわけエネルギー産業分野におけるサイバーセキュリティが取り上げて論じられるのは，同分野を対象とするサイバー攻撃が一企業にとどまらない社会全体への影響をもたらし得る重大性を帯びる可能性を孕み，それだけに攻撃側から見れば魅力的な対象だからである。

実際，エネルギー関連分野におけるサイバー攻撃には下記のような事例がある[3]。

表：エネルギー分野におけるサイバー攻撃事例

	年	発生国	攻撃内容	もたらされた影響
1	2003	米国・カナダ	米国東海岸，カナダ・オンタリオ州の送電システムに対するハッカーによる攻撃	数時間にわたる送電障害
2	2003	米国	オハイオ州デービス・ベッセ原子力発電所でサーバを狙ったSlammerワームが，契約ベンダーが使用するVPN接続を介して侵入・感染	5-6時間にわたる安全管理システムの停止

[1] G7 Energy Ministerial in Hamburg*, Communiqué, G7 Hamburg Initiative for Sustainable Energy Security* (2015), para. 9.
[2] *Ibid*., para. 16.
[3] データについては，Kon Briefing, *Cyber Attacks News Today 2024/2023*, at（https://konbriefing.com/en-topics/cyber-attacks.html）や日本電気株式会社Webサイト「重要インフラに対するサイバー攻撃の実態と分析」at（https://jpn.nec.com/techrep/journal/g17/n02/170204.html）等を参照。

3	2005	日本	従業員の自宅PCがマルウェアに感染し，機密情報がファイル共有ソフト経由で流出	原子力発電所の機密情報流出
4	2007～	米国・英国	英米エネルギー企業5社が数年にわたり中国を発信源とする組織的ハッカーからマルウェアNight Dragonによる攻撃を受ける。	ガス田や入札に関する機密情報の窃取
5	2008	シリア	レーダー網をハッキングした上でイスラエル戦闘機が侵入し核施設を空爆	核施設の破壊
6	2008	トルコ	制御システムに対するサイバー攻撃により石油パイプライン内の圧力上昇	パイプラインの爆発
7	2010	イラン	Natanzウラン濃縮施設におけるSiemens製制御系システムがUSBを介してコンピュータワームStuxnetに感染。米国およびイスラエルによる作戦とされる。	約1,000台の遠心分離機が破壊される。
8	2011	カナダ	複数のエネルギー企業にリモート管理ツールを提供するカナダ企業のネットワークがマルウェアに感染	リモート管理ツールの脆弱性に関する情報が漏洩
9	2012	サウジアラビア	国営石油会社Aramcoのワークステーション3万台がShamoonウィルスに感染	データ消去。内部ネットワークの1週間以上にわたる遮断
10	2012	英国	ロンドン五輪会場の電力システムに対して40分間にわたり1000万回以上の攻撃	実害なし
11	2012	米国	2つの発電所で制御システムがマルウェアに感染	片方は再稼働が3週間遅延，もう一方も運用制限
12	2013	米国	ニューヨーク州ダム管理システムに対する攻撃	一定時間水門を制御される。
13	2014	米国・欧州	Dragonflyハッカーグループによる発電所, 電力系統, 石油パイプライン等を標的としたマルウェアHavexに数百社が感染	多数の情報の窃取
14	2015	ウクライナ	発電所がマルウェアBlack Energy 3に感染	同国西部で数時間にわたる大規模停電
15	2015	トルコ	イランによるサイバー攻撃	各地における12時間にわたる大規模停電

16	2016	ドイツ	原子力発電所の燃料棒監視システムがマルウェアに感染	実害なし
17	2016	イスラエル	電力公社のシステムがフィッシング攻撃によりマルウェアに感染	一部システムが2日間停止
18	2016	ウクライナ	マルウェアIndustroyer/Crash Overrideを用いたサイバー攻撃	キエフ市内1/5が約1時間停電
19	2017	ウクライナ	チェルノブイリ原子力発電所の放射線モニタリングシステムがランサムウェアNot Petyaに感染	手動制御を余儀無くされる。
20	2017	サウジアラビア	発電所の安全システムがマルウェアTritonに感染	実害なし
21	2019	インド	Kudankulam原発管理システムに対するDtrack系マルウェアによる攻撃	データ盗取
22	2020	イラン	Natanz原発に対するサイバー攻撃（＋爆発物の設置)。イスラエルによるとされる。	施設の爆発。核開発計画を1-2年遅らせたと指摘される。
23	2021	イラン	Natanz原発に対するサイバー攻撃。イスラエルによるとされる。	停電。遠心分離機数千台の破壊
24	2021	米国	フロリダ州水道システムに対するサイバー攻撃	水酸化ナトリウム濃度設定が通常の100倍に変更される。
25	2021	米国	従業員のVPN接続用パスワード盗取によりColonial Pipelineがランサムウェアに感染	製油所から東海岸地域への石油パイプラインの数日間の操業停止。75ビットコイン（500万ドル相当）の支払いによりネットワークへのアクセスを回復
26	2022	ウクライナ	ロシアと関係があるとされるサイバー集団Sandwormによる電力監視制御システムおよび送電網に対するサイバー攻撃	ロシア軍の軍事行動に合わせた停電惹起

上記諸事例の中には，攻撃の発信源が国家によるとされるものと非国家主体によるものとがある。また，被害法益に着目しても，企業の機密情報の窃取，停電等による社会経済への影響，さらにはより深刻な大規模損害が発生する恐れがあった例が含まれており，その性質は多様である。これらの多様なサイバー攻撃に対して，国際法はどのように適用されるだろうか。本稿は，主としてエネルギー分野におけるサイバー攻撃を想定してサイバー空間における国際法の適用に関する議論状況や課題について概観する。

Ⅱ　サイバー攻撃の法的評価と対応措置

１．既存の国際法の適用の適否

サイバー攻撃に対して国際法をいかに適用して対処すべきかを巡っては，2000年代に入って議論が本格化した。国連は，2004年に，サイバー空間での責任ある国家の行動に関する政府専門家による議論の場として「サイバーセキュリティに関する国連政府専門家会合（国連サイバーGGE）」を総会第1委員会の下に設置した。同会合は，後述のように，2021年の最終報告書に至るまで数次にわたり報告書を作成している。

他方，NATOサイバー防衛協力センター（CCDCOE: Cooperative Cyber Defence Centre of Excellence）は，2017年に「タリン・マニュアル2.0」を公表した。同マニュアルは，個人資格で議論に参加した研究者・実務家によって作成されておりNATOの公式見解を示したものではないが，非公式に多数の国および国際組織から見解を聴取しつつ作成された経緯もあって，この分野における標準的な文書として広く参照されている。

また，上記国連サイバーGGEにはすべての加盟国が参加していたわけではないこともあって[4]，国連においては，全加盟国および国際組織やNGO等の関係ステークホルダーが広く参加可能な議論の場として，国連オープン・エンド作業部会（Open-ended Working Group（OEWG））が2019年に別途召集され，2021年には国連総会に最終報告書を提出している。

本稿では，サイバー攻撃に関する国際法の規律の現状と課題について，これら諸文書を参照しつつ整理するが，その前提として，国連における当初の議論においては，サイバー攻撃という新たな事象に対してそもそも既存の国際法枠組みを適用して対処すべきか自体が問われたため，この点について確認する。

当初，米国やヨーロッパ諸国，オーストラリアおよび日本は，サイバー攻撃に関して新たな条約の締結や法の「再発明」は不要であり，既存の国際法を適用すれば足りるとし，これに対して中国・ロシア等は新たな規範が必要であると主張していた。両陣営の対立の焦点は，米欧日豪が既存のインターネット利用の自由やプライバシーの保護，民間ガバナンスの原則

[4] 国連サイバーGGE第6会期の委員は25カ国出身の政府専門家で構成された。

を重視するのに対して，中ロが国家によるインターネットの管理強化（いわばガバメント）を正当化する新たな規範の創出を目的とした点にあったとされる。ロシアが国連サイバーGGEというフォーラムがすでに存在した中でOEWGの開催を主導したのも，GGEでは新たな規範の作成について否定的な見解が多数を占めたため，新規範作成のための議論を改めて惹起する意図があったという[5]。

この対立については，国連サイバーGGE第3会期報告書（2013年）が，「平和・安全を維持し，開放的・安全・平和でアクセス可能なICT環境を推進するために，国際法，とりわけ国連憲章は［ICT活動に］適用されるし，その重要性は否定できない（is applicable and is essential）」[6]との参加国のコンセンサスを示したことで一応の決着をみた。国連サイバーGGE第4会期報告書（2015年）および第6会期報告書（2021年）も，この点を再確認している[7]。その上で，第4会期および第6会期報告書では，「責任ある国家行動に関する規範，規則および原則（norms, rules and principles）」と「国際法（international law）」について章を分けて取り上げ，後者においてより具体的に国際法がどのようにサイバー活動に適用されるかに関して一歩踏み込んだ規定を設けた。第6会期報告書は概要以下の点をGGEのコンセンサスとして掲げている[8]。

(a) ICTの利用をめぐる国際紛争の当事国は，国連憲章2条3項および第6章に従い，憲章33条に定める諸手段を通して平和的に当該紛争の解決を図らなければならない。
(b) 国家主権および主権に由来する国際規範および原則は，国家によるICT関連活動および国家領域内のICTインフラに対する管轄権行使に関して適用される。既存の国際法上の義務が国家のICT関連活動に適用される。国家は，自国領域内のICTインフラに対して，とりわけ，政策と法令を整備し，ICT上の脅威からこれらインフラを保護するために必要なメカニズムを構築することを通して管轄権を行使する。
(c) 不干渉原則に従って，国家はICT技術を用いて他国の国内管轄事項に対して直接的にあるいは間接的に干渉してはならない。
(d) ICTの利用においては，国連憲章に従って，武力の行使または武力による威嚇を控えねばならない。
(e) 国家は国際法に従い国連憲章で認められた措置をとる固有の権利を有する。この点についてはさらなる研究を要する。

---

[5] 赤堀毅『サイバーセキュリティと国際法の基本—国連における議論を中心に—』（東信堂，2023年）11-12頁。

[6] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98*, para. 19.

[7] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174*, para. 24; *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135*, para. 69. なお，第5会期は報告書の採択に至らなかった。

[8] *Ibid.,* para. 71.

(f) 国際人道法は，武力紛争時においてのみ適用される。人道，必要性，比例性，区別原則等が，ICT利用に関してどのように適用されるかについてはさらなる研究を要する。

(g) 国家は国際法上自国に帰属される国際違法行為に関して義務を果たさなければならない。国家は，私人に国際違法行為を行わせてはならず，また自国領域が非国家主体によって違法行為に使用されないように努めなければならない。もっとも，ICT上の行為が領域内で行われたことのみでは当該行為は国家に帰属せず，国家が違法行為を組織・実行したという主張は立証されなければならない。

国連OEWG最終報告書（2021年）も，GGE第4会期報告書が国連総会によって確認され，ICT利用の枠組みを確立したことに触れ，OEWGもこの基礎に立脚することを謳った[9]。

このように，国連での議論を経てサイバー活動に対しても既存の国際法規範の適用が肯定されるに至った。他方で，後述するように，より具体的にこれら諸原則をサイバー攻撃にいかに適用し得るかについてはサイバー活動の特質に応じた種々の争点が存在する。では，具体的にはどのような議論がなされ，どういった課題が存在するのだろうか。以下では，サイバー攻撃を分類しつつ，それぞれの類型に当たる事態を想定して国際法の適用のあり方を検討しよう。

２．武力攻撃／武力行使に該当するサイバー攻撃への対応

(1) 武力攻撃

国際法上，「武力攻撃（an armed attack）」に対しては，自衛権行使によって武力を用いて対応することが認められる。サイバー攻撃との関係では，まずサイバー上の攻撃が「武力攻撃」に当たるかが問題となるが，対象国においてその「規模と効果」の観点から一定の閾値を超える物理的破壊をもたらすサイバー攻撃は，武力攻撃に該当し，自衛権行使の対象となると一般に解されている[10]。日本においても，「どのようなサイバー攻撃であれば武力攻撃に当たるかについては，その時点の国際情勢，相手方の明示された意図，攻撃の手段，態様等を踏まえ，個別の状況に応じて判断すべきものと考えています。その上で，一般論として申し上げれば，サイバー攻撃のみであっても，例えば，物理的手段による攻撃と同様の極めて深刻な被害が発生し，これが相手方により組織的，計画的に行われている場合には武力攻撃に当たり得ると考えられます」との国会答弁が示されているところである[11]。

---

[9] *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, A/AC.290/2021/CRP.2*, paras. 7-8.

[10] Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2017), p. 339; Ise-Shima Summit, *Communiqué, G7 Principles and Actions on Cyber* (2016), p. 1.

[11] 安倍晋三総理大臣答弁，第198回国会衆議院本会議会議録 第24号（令和元年5月16日）13頁。

ただし，個別状況を強調する上記答弁も示唆するように，武力攻撃に該当する「規模と効果」の具体的な閾値について国際社会に一致した見解があるわけではない。米国防省が作成した『戦争法マニュアル』では，例えば，原子力発電所のメルトダウンを引き起こす攻撃，人口密集地域の上流に位置するダムを決壊させる攻撃，航空管制システムに不具合を生じさせ航空機を墜落させる攻撃等が武力攻撃に含まれ得るとしており[12]，大規模な物理的損害を引き起こす攻撃を想定しているように思われるが，それ自体で直ちには物理的被害を伴わない軍の命令システムや防空システムの麻痺をもたらすサイバー攻撃がいかに評価されるか等，その外延については明らかではない。また，物理的な攻撃に先んじてサイバー攻撃が実施される場合，いかなる時点で武力攻撃の着手を認めることができるのかも問題となる。例えば，2007年にはシリアに建設中の核関連施設とみられる施設が，イスラエル空軍機の爆撃を受けて破壊されたが（表：事例5），当該爆撃の際，事前にマルウェアに感染させられていたシリアの防空システムはイスラエル空軍機の飛来を探知できなかったという。そうした事例において，いかなる時点で武力攻撃の着手を認め得るのかは問題となろう。もっとも，武力攻撃の「規模と効果」の閾値や武力攻撃の着手時点をめぐっては，サイバー攻撃に限らず一般的にも議論がなされているところであるから，この点については既存の国際法の解釈問題とも評価できる。

他方で，仮に武力攻撃が発生したと評価し得る場合に，これに対する自衛権の行使としてキネティックな武力行使が可能かについては，米欧はこれを肯定し，ロシアはサイバー上の反撃のみが許容されると主張する。この点の合意が得られなかったことはGGE第5会期（2017年）が報告書の採択に失敗した要因の1つとされており，残された課題の1つである。

(2) 武力行使

国際法上，上記の武力攻撃に閾値に達しない「武力行使(use of force)」に対して，被害国が何をなし得るかについても争いがある。タリン・マニュアル2.0は，「規模と効果」においてキネティックな武力行使に匹敵するサイバー攻撃は，国連憲章2条4項で禁止される武力行使に該当するとする[13]。もっともその具体的な閾値について合意はない。例えば，遠心分離機を破壊したStuxnetによるイラン核施設に対するサイバー攻撃事案（表：事例7）は武力の行使に当たると考えられるだろうか。また，ウクライナの原子力発電所の放射線モニタリングシステムを機能喪失に至らしめたNotPetyaによるサイバー攻撃事案（表：事例19）のように，直接の物理的被害を発生させるわけではないサイバー攻撃はどうだろうか。同様に，例えば，銀行・証券システム，航空機・鉄道輸送，年金等の社会福祉制度，保健システム，配電網等に対してなされる物理的損害を生じない攻撃が武力行使に当たるかについて，どういった判断基準を設け得るかが問題となる。

---

[12] U.S. Department of Defense, *Law of War Manual* (2015), para. 16.3.1.
[13] *Tallinn Manual 2.0, supra* note 10, p. 330.

また，仮に上記のようなサイバー攻撃を武力行使と評価し得るとして，これに対して，攻撃を受けた国がいかなる措置を講ずることができるかについても多くの整理すべき点がある。第1に，武力攻撃に至らない侵害に対し，自衛権の行使として必要最小限度の範囲内において武力を行使することが認められるかは一般国際法上も争点となっているが[14]，これをサイバー分野においてどのように解すべきだろうか。第2に，武力行使に対して比例性のある武力を用いた対抗措置をとることができるのかも，ニカラグア事件に関する国際司法裁判所（ICJ）判決をどう読むかを含めて一般国際法上の議論の延長として問題となる[15]。第3に，サイバー攻撃においては攻撃主体が直ちには判明しないことも想定されるが，そうした状況下で攻撃を排除するためにハックバック等を行うことは比例性のある反撃として認められるだろうか。第4に，武力攻撃に至らないサイバー攻撃に対し，反撃措置は，当該サイバー攻撃そのものを排除する限度（on-the-spot-reaction）に限られるか，再発防止を含めたより積極的な措置までとり得るか。第5に，サイバー攻撃に対し，物理的な攻撃で反撃することは可能か。仮に可能であるとして，比例性要件の充足をいかに考えるべきかも問題となる。

３．国家による武力行使に至らないサイバー攻撃への対応

以上のように，どのようなサイバー攻撃が武力攻撃または武力行使に当たるか，それらに対してどのような対応が可能かについては未だ不明確な点が多く議論は続いている。もっとも，実際のサイバー攻撃は，武力行使に至らないと考えられるものが大半を占める。上記の国連サイバーGGE第6会期報告書における国際法原則（c）および（g）からも見てとれるように，そうしたサイバー行動が国家に帰属し，かつ違法な干渉に当たる等の理由によって国際法違反を構成すれば，攻撃国の国家責任が発生する。干渉とは，国家がその主権に基づいて自由に決定すべき事項に対して，他国が強制的な方法を用いて関与することを指す[16]。サイバー手段を使用した脅迫によって，他国にその意思に反して何らかの行為を行わせる行為等は典型的な干渉に当たろう。もっとも，サイバー行動の国家への帰属を立証することは往々にして困難であり，また，仮に立証できる際にも探知能力・手法を秘匿するために立証過程の詳細を明かすことに躊躇する国も多いとされる[17]。

---

[14] 武力攻撃に至らない武力行使に対する自衛権行使の可能性について，東郷和彦外務省条約局長答弁，第143回国会衆議院外務委員会会議録第4号（平成10年9月18日）14頁。

[15] ニカラグア事件本案判決は，仮にニカラグアがエルサルバドル等に対して武力行使を行なっていたとしても，これに対しては被害国による比例性のある対抗措置のみが正当化されるのであり，第三国である米国による，とりわけ武力行使を含むニカラグアに対する介入は正当化されないとするが（*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, *Merits, I.C.J. Reports 1986*, p. 127, para. 249），当該判示は被害国による武力を伴う対抗措置を肯定する趣旨かが争われてきた。

[16] *Ibid.*, pp. 107-108, para. 205.

[17] サイバー行動に関する立証問題については，Sharngan Aravindakshan, “Cyberattacks: A Look at Evidentiary Thresholds in International Law,” *Indian Journal of International Law,* Vol. 59 (2021), pp. 285-299.

仮に国際法に反するサイバー行動が国家に帰属することを立証し得た場合には，国家責任が生じ，当該国が違法行為を行ったことを認めて違法なサイバー行動を停止し，発生した損害を賠償すれば事態は解決に向かう。しかし，違反の事実や責任を国が認めない場合には，被害国には一定の条件の下で対抗措置に訴えることが認められることになる。対抗措置についてはGGE報告書では明記されなかったが，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（2017年）は，「国際違法行為の被害者である国家は，一定の場合には，その違法行為について責任を有する国家に国際的な義務を遵守させるために，当該責任を有する国家に対して均衡性のある対抗措置（ICTを介して実施する措置を含む）及びその他の合法的な対応をとることができる」とする[18]。タリン・マニュアル2.0規則24も同様に被害国が対抗措置をとることを肯定している[19]。

サイバー攻撃に対して被害国がサイバー上の対抗措置をとる場面を想定すると，各国の技術的差異が問題となる可能性がある。一般国際法上，第三国による対抗措置が可能かについては議論があるが，例えば，サイバー攻撃を受けた国が，法的には均衡の取れた対抗措置を講じ得るにもかかわらず，そのためのサイバー関連能力を有しない場合，第三国による技術的援助が可能か否かは問題となろう。

４．非国家主体によるサイバー攻撃への対応

(1) 相当の注意義務を介した国家責任追及

サイバー攻撃が非国家主体によって行われたとしても，これがいずれかの国家の指示による場合もある。もっとも，侵害行為の国家への帰属を証明することは往々にして困難である。また，そもそも国家の意思とは関係なく私的主体がサイバー攻撃を行うことが実際には多い。これらの場合において，非国家主体の行為自体の国家への帰属を証明できなくとも，「国家は，領域主権の行使により，その国家領域をみずから使用しまたは私人にその使用をゆるすにあたっては，他国の領域その他の国際法上の権利を害する結果にならないよう，一般国際法上，特別の注意義務を課される」[20]とする「領域使用の管理責任」に基づいて，侵害行為に利用されるサイバーインフラが領域内に所在する領域国に相当の注意義務を負わせることを介して関係国の国家責任を問うことができないかが議論されている。

上記の国連サイバーGGE最終報告書は，国際法原則(g)において領域管理責任に言及するが，「国家は自国領域が非国家実体によって国際違法行為のために使用されないよう確保に努める（should seek to ensure）」として，法的義務性については曖昧な書き振りをとっていた。これは，領域使用の管理責任に基づく「相当の注意義務」が国家に過大な負担を強いることを危

[18] G7 Foreign Ministers' Meeting in Lucca, *G7 Declaration on Responsible States Behavior in Cyberspace* (2017), p. 2.
[19] *Tallinn Manual 2.0, supra* note 10, p. 130.
[20] 山本草二『国際法〔新版〕』（有斐閣，1994年）275頁。

惧する国があったためであるが，ジェノサイド防止義務についてさえ，ICJは「自国にとり得る（within its power）すべての措置をとったか」という枠組みで判断をしていることからもわかるように[21]，相当の注意義務は，国家に合理的に要求し得ないことまで要求しない。領域国は自国のサイバー能力の範囲内において，自国領域内の非国家主体が他国・他国民に対してサイバー攻撃を行わないように相当の注意を払えば良いことになる[22]。

タリン・マニュアル2.0においては，規則6および7に相当の注意が義務として規定されている。規則6は，「国家は自国領域や自国のコントロール下の領域ないしサイバーインフラが他国の権利に影響を与えこれに深刻な結果をもたらすように利用されないように相当の注意を払う義務がある」[23]とする。ここでは義務性が確認された上で，領域に加えて管轄下の行動も対象に加えられている。その上で，規則7は，「相当の注意原則は，他国の権利に影響し，深刻な結果をもたらすサイバー活動を停止させるために，状況において可能なあらゆる手段をとることを国家に要求する」[24]とその内容を具体化し，求められる注意の程度が対象国のサイバー能力によって変わり得ることを確認する。

なお，領域使用管理責任については，サイバー空間の連接性から，サイバー空間を介した侵害行為の経由国がどのような責任を負うかが問題となる。仮に各国がその領域内のサイバーインフラを通過するだけの侵害行為に対して責任を持つとして，その場合の責任は侵害行為の発信源が所在する国と同程度か等については検討が必要であろう。

(2) 非国家主体に対する管轄権行使

非国家主体によるサイバー攻撃に対しては，これを特定の国家と結びつけるのではなく，私人による犯罪行為として捉え刑事処罰を行うという対応も考えられる。この場合，複数国が関係し得るというサイバー犯罪の特徴に応じて，いずれの国が捜査や訴追等の管轄権を行使し得るかが問題となる。

このうちサイバー上の捜査活動については，2001年に締結されたサイバー犯罪に関する条約（サイバー犯罪条約：ブダペスト条約）およびその附属議定書（コンピュータ上のヘイトクライムに関する2003年第1追加議定書；協力強化および電子的証拠の開示に関する2021年第2議定書）が一定の規律を定めている。もっとも，同条約は，データにアクセスする権限を持つ者の「合法的なかつ任意の同意」がない場合に，他国領域内のコンピュータに蔵置されているデータに越境アクセスを伴う捜査をなし得るかについて，条約策定時には実行が少なく

---

[21] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, *I.C.J. Reports 2007*, p. 221, para. 430.
[22] サイバー攻撃と相当の注意義務について詳しくは，拙稿「サイバー・セキュリティ事案における『相当の注意』義務」浅田正彦ほか編『現代国際法の潮流II』（東信堂，2020年）301-316頁参照。
[23] *Tallinn Manual 2.0, supra* note 10, p. 30.
[24] *Ibid*., p. 43.

不明確であるとして規定を置かなかった[25]。また，「犯罪が自国の領域内で行われる場合」に当該国による裁判権行使を想定するが（22条1(a)），そもそもサイバー上の行為については，いずれの国の領域で発生したか自体が解釈問題となる。さらに，同条約の当事国は2024年5月末現在で72カ国であるから，非当事国が行う，あるいは非当事国に所在するデータに関する越境捜査やサイバー犯罪の訴追は，いずれにせよ一般国際法に基づいて評価すべき問題となる。

では，一般国際法上，サイバー犯罪に対する管轄権行使はどのように理解すれば良いか。第1に，一般国際法上，犯罪捜査等を含む執行管轄権は，外国領域において行使できないとされる。国連サイバーGGE最終報告書の国際法原則(b)では，「国家領域内のICTインフラに対する管轄権行使」への言及がある。確かにサイバーインフラに着目すれば，それが設置されている領域国を特定することができ，当該国の同意なしにサイバーインフラにアクセスし証拠収集等の執行管轄権を行使することは違法な執行管轄権行使の域外適用と考えることもできるかもしれない。しかし，サイバー犯罪の捜査において主たる捜索対象となるのは物理的な機器自体というよりもデジタルデータであろう。とりわけ，クラウド上のデータについては，いずれの国家内のストレージに所在するかは往々にして不明であるし，複数国に所在する複数のストレージに分有されていることも多く，特定の「領域国」との結びつきは希薄である。外国領域における執行管轄権行使が禁止される理由が，領域国の排他的統治権を害することの禁止にあるとすれば，そもそも特定の領域国の管轄と排他的に結びついていないという側面を持つデジタルデータについては，執行管轄権行使の限界をどのように捉えれば良いのかという問題が浮上するのである[26]。

第2に，域外で行われたサイバー犯罪の訴追については，立法管轄権およびこれを前提とした司法管轄権行使の射程の問題となる。立法管轄権の行使範囲については，当該国が事案の性質に照らして密接な関連を持ち管轄権を行使することが合理的かという枠組みで捉えることができる[27]。その際の考慮要因の1つとして，管轄権行使が他国の政策実現を害する程度が検討されるが，この点については国家がそもそもサイバー活動について持つ管轄権の内容が関係する。例えば，関係する国の間でサイバー政策に根本的な差がなく，問題となるサイバー犯罪を訴追することを等しく望むのであれば，訴追の意思と能力を持つ国がこれを行うこともサイバー犯罪の国際的な抑圧という観点からは合理的と考える余地が生じるだろう。

---

[25] Council of Europe, *Explanatory Report to the Convention on Cybercrime* (2001), para. 293.
[26] 詳しくは，拙稿「越境サイバー対処措置の国際法上の位置づけ」国際法研究14号（2024年）62-67頁。
[27] 国家管轄権に関する考え方については，拙稿「国家管轄権の『域外適用』再考」日本エネルギー法研究所編『エネルギーに関する国際取決めの法的問題の諸相－2017～2018年度 エネルギーに関する国際取決めの法的問題検討班報告書－(JELI-R-No.154)』（2023年）143-158頁。

Ⅲ　サイバーセキュリティの回復措置

以上に確認したように，サイバー攻撃に対しては，それが武力攻撃に当たれば自衛権行使による対応が認められ，武力攻撃に満たない武力行使に対しては武力によって対抗することの是非およびその根拠について議論が続いている。国家に帰属するサイバー攻撃や国家が領域国としての管理責任を怠った結果発生したサイバー攻撃に対しては，当該国の国家責任を追及し，対抗措置をとることが想定され，サイバー攻撃を行なった私人を犯罪者として処罰することも考えられる。

もっとも，責任追及や関係者の処罰といった後者の措置は事後的な対応にとどまる点で限界を有する。対抗措置も違反国に対して責任を認めて賠償を行うように，あるいは相手国が義務違反や責任を認めないのであれば，適切な紛争解決手続を利用するように圧力をかける間接強制としての性質を持つものである。これに対して，サイバー攻撃が続いている場合には，まずはこれを遮断し，サイバーセキュリティを回復することが現実にはより重要であろう。その一環として，外国に所在する攻撃発信元に対してハックバック措置をとることが，領域国の管轄権を侵害する場合は，国際法上はそうした対応措置が緊急避難として例外的に正当化されるかという問題となる。

国連国際法委員会が作成した国家責任条文25条は，「重大かつ差し迫った危険（a grave and imminent peril）」から「根本的利益（an essential interest）」を守るために，国は緊急避難を援用して行動できることを規定しているが，サイバー空間を通じた侵害のうち，いかなるものが上記に該当すると考えられるだろうか。緊急避難について定めるタリン・マニュアル2.0規則26に付されたコメンタリーは，「根本的利益」について国際法上定まった見解はないとしつつも，防空システム，銀行・証券システム，航空機・鉄道輸送・電力供給等に関するインフラ，社会福祉・保健制度といった，国の安全保障・経済・公衆衛生・治安・環境等を支える重要インフラに深刻な被害が生じた場合をその例として挙げる[28]。

では，そうした重要インフラへのサイバー攻撃に直面した国は，攻撃元コンピュータ等に対してどのような範囲でハックバック措置をとることができるだろうか。国家責任条文26条では，緊急避難の法理によっても，強行規範たる武力不行使原則違反を正当化することはできないとされているが，タリン・マニュアル2.0においては，武力を用いた緊急避難措置が許されるか否かについて，合意に至らなかったとされる。サイバー攻撃を阻止する方法として，発信源のサイバーインフラを破壊することが不可欠であり，当該措置が武力行使と見做される場合，緊急避難によってそうした措置が正当化され得ると解するのかが問題となる。また，第三国に所在するサイバーインフラを経由してサイバー攻撃が行われ，当該攻撃を排除するためには，当該第三国に所在するサイバーインフラを破壊する必要がある場合，サイバー攻

[28] *Tallinn Manual 2.0, supra* note 10, p. 136.

撃の被害国は，緊急避難を援用して当該インフラを破壊することができるかも問題となろう。

Ⅳ　むすびに代えて

本稿は，サイバー攻撃が発生した場合を念頭に置いて，国際法上，そうした攻撃がどのように評価され，被害国にはいかなる対応が認められるかについて整理した。その結果，サイバー攻撃とそれへの対応は，概ね既存の国際法の枠組みに照らして位置づけ得ること，しかし，サイバー上の攻撃とこれへの対応であることの特質に起因して解釈・適用上の多くの課題が存在することが確認された。

上記の国際法上の枠組みは，基本的にサイバー攻撃を受けた国家による対応を中心に構築されている。もっとも，エネルギー産業に対するサイバー攻撃は，まず第一に事業者に対して向けられるものである。サイバーセキュリティの維持・回復における事業者の役割はどのように位置づけられるだろうか。むすびに代えて，日本におけるサイバーセキュリティ対策を概観することを通して，この点について最後に確認しよう。

日本においては，2014年にサイバーセキュリティ基本法（平成26年法律第104号）が採択された。同法は，「国民生活及び経済活動の基盤であって，その機能が停止し，又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者」を「重要社会基盤事業者」と位置づけ（3条1項），これら事業者に対して，「基本理念にのっとり，そのサービスを安定的かつ適切に提供するため，サイバーセキュリティの重要性に関する関心と理解を深め，自主的かつ積極的にサイバーセキュリティの確保に努めるとともに，国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努める」ことを義務づける（6条）。また，政府は，重要社会基盤事業者におけるサイバーセキュリティの確保の推進に関する事項を含むサイバーセキュリティ戦略を定めることとされ（12条），重要社会基盤事業者におけるサイバーセキュリティに関し，基準の策定，演習および訓練，情報の共有その他の自主的な取組の促進その他の必要な施策を講ずることも国の責務として定められた（14条）。同法に基づき，内閣サイバーセキュリティセンター（NISC）では，サイバーセキュリティ戦略および重要インフラのサイバーセキュリティに関する行動計画等を作成し，サイバーセキュリティの確保を事業者に促している[29]。同行動計画では，情報通信，金融，航空，空港，鉄道，電力，ガス，政府・行政サービス，医療，水道，物流，化学，クレジット，石油および港湾を重要インフラサービスと位置づけ，これらに関与する事業者をサイ

[29] 最新の行動計画等については，NISC Webサイト（https://www.nisc.go.jp/policy/group/infra/index.html）を参照。

バーセキュリティ上の重要社会基盤事業者（重要インフラ事業者）と指定する[30]。重要インフラ事業者には行動計画に沿った一定のサイバーセキュリティ対策が求められることになる[31]。

電力分野においては，「事業用電気工作物を設置する者は，事業用電気工作物を主務省令で定める技術基準に適合するように維持しなければならない」と定める電気事業法39条1項を受け，電気設備に関する技術基準を定める省令15条の2が，「事業用電気工作物（小規模事業用電気工作物を除く。）の運転を管理する電子計算機は，当該電気工作物が人体に危害を及ぼし，又は物件に損傷を与えるおそれ及び一般送配電事業に係る電気の供給に著しい支障を及ぼすおそれがないよう，サイバーセキュリティ（サイバーセキュリティ基本法（平成26年法律第104号）第2条に規定するサイバーセキュリティをいう。）を確保しなければならない」とする。

セキュリティ対策としては，日本電気技術規格委員会（JECS）が定めた「電力制御システムセキュリティガイドライン」（2016年）や「スマートメーターシステムセキュリティガイドライン」（2016年）が存在し，また，2017年には電力ISAC（Information Sharing and Analysis Center）（JE-ISAC）が設立された。電力ISACは，電力10社，大規模発電業者等27社，日本卸電力取引所および電力広域的運営推進機関で構成され，セキュリティインシデントやベストプラクティスに関する情報共有を行っている。さらに，2018年には日欧米でMOUを締結し連携して情報収集・分析に当たっている。

上記の電力インフラのサイバーリスク対策は，基本的に平時におけるサイバーセキュリティの維持を念頭に置いて，サイバー攻撃に対する耐性を高める事業者の責任を定めている。もちろん，サイバー攻撃の大部分は，私人によって平時に行われる犯罪行為であり，これに対して備えることは極めて重要である。しかし，表（事例7，15，22，23，26）でも見たとおり，電力インフラは有事を含め外国からの攻撃対象となることも想定される。そうしたリスクに対して，事業者と国の責任分担をどう考えるのかは今後の課題であろう。仮に事前防護措置をとったにも関わらずサイバー攻撃の被害に遭った際に，国と事業者の間で対応措置や生じた損害に対する費用負担等はどのように分担すべきだろうか。より具体的には，例えば，サイバー攻撃を受けた際に，事業者としては，事業内ネットワークを外部から遮断したり，侵入されたウィルスを駆除したりしてさらなる被害を防ぐことは当然として，攻撃元の特定や証拠収集，盗取されたデータの無効化等のためにハックバック措置をとることも認められるべきだろうか[32]。また，自前で十分なサイバーセキュリティ対策をとる体力のない事業者や

---

[30] サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」（2022年6月17日）別紙1。

[31] 重要インフラ事業者が取り組むべき事項について詳しくは，同上，36-37頁。

[32] 米国では，2019年に，民間のサイバー攻撃被害者が自ら自己ネットワーク外でのハックバック措置をとることを正当化するActive Cyber Defense Certainty Act法案が提出されたが（法案については，https://www.congress.gov/bill/116th-congress/house-bill/3270参照），正確なトラックバックが行われない可能性や第三者に被害を与えた場合の対処，正当な自衛の範囲の確定等の難点から廃案となっている。Jen Ellis, “Hack Back is Still Wack,” at（https://www.rapid7.com/blog/post/2021/08/10/hack-back-is-still-wack/）.

能力があっても十分な対策を取らない事業者が攻撃対象となった場合，これら事業者の責任をどう解するべきか。サイバーセキュリティ対策についての議論が進む米国では，権限を持つ連邦政府とサイバー対応能力を持つ事業者を含む私的セクター間の協働によって攻撃に対処する必要性が強調されているが[33]，日本においても国と事業者の責任分担のあり方についてより詳細な検討が望まれる。

（追記）本稿脱稿後に、中村和彦『越境サイバー侵害行動と国際法――国家実行から読み解く規律の行方――』（信山社、2024年）に接した。また、第217国会（2025年）において「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」が可決・成立し、日本においても官民間の情報共有によるサイバー攻撃事案の未然防止、対処支援強化等が図られるに至った。

[33] The White House, *National Cybersecurity Strategy* (2023), p. 15.