（要約）

越境サイバー侵害行動に対する国際法の適用をめぐる国家実行の評価

中　村　　和　彦

Ⅰ　はじめに

2000年代以降その多大な損害・損失が顕在化してきたサイバー攻撃に関し、国際社会はこれに多数国間条約の作成により対応しようとしてきたが、交渉・改正等に時間を要する上、越境サイバー攻撃に関与する国々を取り込むことによりむしろ国際協力の可能性を狭めるルールに帰着しかねないジレンマがある。

かかる認識の下、本稿では、特に各国の関心が高く国連等で議論の対象となっている、国境を越えて敢行され、国家又は国家に準ずるテロ組織等の関与・支援が疑われるサイバー攻撃であって、被害国の政治的・経済的・社会的基盤に広範な人的・物的・経済的損害又は国家としての基本的機能への侵害をもたらすもの（以下「越境サイバー侵害行動」という。）に対処するため、各国が慣習国際法を含む現行の実定国際法のどの規範を、どのように適用しようとしているか、今後のあり得べき国家実行の方向性を含め、各国の公式の立場表明・国家実行等から考察する。一個人・組織のレベルのサイバー攻撃への対処は、検討対象から除く。サイバー空間における人権侵害は、別途包括的に検証すべき重要な課題なので、本稿の検討対象とはしない。

Ⅱ　一次的規範（保護法益）

1　各国の立場表明

各国が自ら公表する越境サイバー侵害行動に対する国際法の適用に関する立場表明、国連の政府専門家グループ（ＧＧＥ）、オープン・エンド作業部会（ＯＥＷＧ）等に各国が見解を示した提出文書、ＧＧＥ・ＯＥＷＧが作成しコンセンサスで採択された報告書は、越境サイバー侵害行動に対する慣習国際法規範の適用に関する各国の法的確信、あるいは条約規範の適用につき「当事国の間で後にされた合意」、「解釈についての当事国の合意」ないし「後に生じた慣行」の存在又はその萌芽を示す有力な材料と評価される。

これらの立場表明・報告書等を検証すると、越境サイバー侵害行動に対して適用される実定国際法の一次的規範、換言すれば、越境サイバー侵害行動がいかなる国際法上の保護法益を侵害するかに関し、武力による威嚇・武力の行使の禁止及び国内管轄事項への不干渉義務が適用され得ることについては、広範な諸国に共通の法的確信が確立しつつある。

これに対し、他国の（領域）主権侵害の禁止及び領域国（加害行為地国）の相当の注意義務の越境サイバー侵害行動への適用に関しては、米国・英国が慣習国際法としての性格に否定的な見解又は一定の留保を示している。もっとも、米国は、主権との関連で、武力の行使や不干渉義務の敷居を下回る一定の越境サイバー活動が国際法違反となる場合があることは認めている。また、英国も、不干渉義務について、議会の運営や金融システムの安定への干渉等、従来よりも幅広い範疇のサイバー侵害行動が違反を構成し得るとの立場をとっていると解される。したがって、これらの国々を含め、従来一般に認められてきた不干渉義務違反の要件を満たさない越境サイバー侵害行動について何らかの国際法違反が成立し得るとの認識は共有されつつある。

相当の注意に関しては、米国・英国とも、関連するＧＧＥの自主規範の指針の意義を認め、これ

を支える国家実行が未だ成熟していないことを指摘している。また、「相当の注意」の外縁が明確性を欠くとの指摘があり、中国、ロシア、開発途上国等は立場を明示的に表明していないが、これらの国々の多くは主権の重要性を強調しており、領域主権の排他性の論理的帰結である「相当の注意」の責任ないし義務自体は否定し難いと考えられる。

国際人道法に関しては、特に非国家主体により通常兵器を伴わない越境サイバー侵害行動のみが単独で行われる場合が武力紛争に該当し得るかについて各国の見解が分かれ、各国間の議論が「どのように」適用されるかの各論にまで及んでいない。

2　国家実行又は後に生じた慣行

上記1において確認された規範認識が越境サイバー侵害行動事案に適用のある規範として認められるためには、それらを越境サイバー侵害行動の具体的な事案に実際に適用した広範な国家実行ないし「後に生じた慣行」の蓄積を示す必要がある。

この点に関し、これまで、武力による威嚇・武力の行使、国内管轄事項への不干渉、他国の（領域）主権侵害の禁止、領域国の相当の注意義務、国際人道法のいずれについても、各国が実際にその違反を明示的に認定した事例は確認されない。各国が国際法違反の認定を回避している背景には、サイバー行動の着手の簡便性、即時（即効）性、匿名性等ゆえに、その侵害国への帰属（attribution）の認定・立証が困難であることがある。

しかしながら、各国の立場表明と個々の越境サイバー侵害行動事案への対処事例とを併せて総合的に分析すると、広範な諸国の間で、越境サイバー侵害行動が情報通信、医療、金融、エネルギー等の重要インフラ又は国の公的機関の物理的損害又は機能の喪失をもたらす場合には何らかの国際法上の義務に反し得るという規範認識の下、これらの類型に該当し得る越境サイバー侵害行動事案について、関係国が国際法違反かどうかの明示を避けつつも、他国又は他国と密接な関連を有する個人・団体に帰属することを政府の公式声明、国内刑事手続等により認定した次のような事例が看取される。

(1)　米国 Sony Pictures Entertainment 社へのサイバー攻撃・脅迫（2014 年 11～12 月）、バングラデシュ銀行に対するサイバー強盗（2016 年 2 月）等

(2)　ランサムウェア（「身代金」要求型ウイルス）WannaCry による世界規模の攻撃・被害（2017 年 5 月）

(3)　ランサムウェア NotPetya によるウクライナ等世界各地のデータ破壊・システム停止等（2017 年 6 月）

3　考察

武力による威嚇・武力の行使の禁止に関し、エストニアへの大規模な DDoS 攻撃（2007 年 4 月）、イランの核燃料濃縮施設に対するマルウェア Stuxnet による攻撃（2010 年夏）、ロシアによるウクライナ侵略の直前・直後に発生したウクライナの電気通信事業者、政府機関、商業衛星通信ネットワーク等に対する相次ぐサイバー攻撃（2022 年 1 月～3 月）のいずれの事案についても、広範な機能喪失や物理的損壊が発生し、被害国は攻撃に関与した国を公に特定していたにもかかわらず、違法な武力の行使ないし武力攻撃と認定していない。このことから、広範な機能喪失や物理的損壊を伴う越境サイバー侵害行動を受けた各国が、実際に武力攻撃の水準に達したと認定して自衛権を行

使する事例は、今後も極めて稀であろうと予想される。

国内管轄事項への不干渉に関しては、多くの国・学説が、越境サイバー侵害行動について「強制」の要件を立証・認定することが困難としている。例えば、米国民主党全国委員会（DNC）のハッキング・情報漏洩事案（2016 年 6～7 月）では、大統領選挙への干渉の可能性が指摘され、米国政府がロシアの関与を公に認定したにもかかわらず、不干渉義務違反を認定するには至っていない。

その一方で、先述のとおり、重要インフラ又は国の公的機関の物理的損害又は機能の喪失をもたらす越境サイバー侵害行動について何らかの国際法違反を認定すべきとの認識が、広範な諸国の間で共有されつつある。各国がこの認識に該当する事案について、次のア、イいずれかの方法で国際法違反の認定を行う実行に繋がり、不干渉義務、主権侵害の禁止のいずれかの国際法規範に違反するという「緩やかな」規範認識が定着していく余地はあろう。

ア　国内管轄事項への不干渉義務違反の認定における「強制」要件の判断基準の実質的な緩和・調整

「強制」を、侵害国の故意により被侵害国から管理ないし主権の行使における自由意思を剥奪することを目的とする圧力と定義し直す等。

イ　他国の（領域）主権侵害の判断基準の明確化

学説上検討されている越境サイバー侵害行動による主権侵害の 2 つの判断基準、すなわち①被侵害国の領土一体性に対する侵害の程度、②本質的に政府に属する機能への干渉又は当該機能の侵奪の有無のうち、②については主権の侵害に該当することで概ね一致が見られる一方、①に関しては、(i) 物理的な損壊・死傷を伴う場合、(ii) 機能の喪失を伴う場合、(iii) 機能の喪失に至らない場合の 3 段階のうち、特に (iii) が主権の侵害に該当し得るかどうかについて見解が分かれている。

①に関しては、(i) 及び (ii) のうち重要インフラ又は国の公的機関の物理的損害をもたらす越境サイバー侵害行動について、主権の侵害に該当することにつき、広範な諸国の支持を得られる可能性がある。これ以外の場合については、なお主権侵害の該非が明らかでない「グレイゾーン」の状況が続くと見込まれ、特に、物理的損壊・機能の喪失もデータ・通信の改変も伴わない端末・システムへの侵入等に関しては、諜報活動を国際法上違法とはしない立場をとる国が少なくないことから、広範な諸国が主権の侵害と認めることで一致する可能性は乏しい。

②に関しては、執行管轄権の行使のための他国に所在するデータへのアクセスについて、当該データがインターネット上等で公に利用可能である場合、及び会員制のオンライン広場等、公に利用可能ではないものの（ログイン ID・パスワードの申請・入手等により）執行国内に所在する不特定多数の個人が利用することができる場合には、他国の主権を侵害する領域外への執行管轄権の行使には当たらないとする学説上有力な見解が、各国間でも徐々に多数派となっていく可能性があろう。

領域国の相当の注意義務に関しては、行為の国家への帰属の立証に伴う負担・困難が相当程度軽減されるので、その射程について広範な諸国間で認識が明確化・共有され、非国家の個人・団体による越境サイバー侵害行動について違反を認定する素地が整うことが、今後の国家実行の蓄積の鍵となる。学説及び上述のＧＧＥの自主規範の指針に関する議論・実行に加え、信頼醸成措置及び能力構築を通じ、各国で重大サイバー事案の連絡窓口（PoC）の指名、コンピュータ緊急事態対応チーム（CERTs）の設置・強化、法的能力構築等の取組が進めば、将来的には、全ての国連加盟国間で共通の「相当の注意」の具体的内容が明確化されていく素地が十分にあると考えられる。

国際人道法に関しては、少なくとも、軍の正規の構成員が通常兵器による軍事行動と連携して越

境サイバー侵害行動を行う場合に適用されることについては、比較的早期に各国の法的確信の収斂が見込まれる一方、この範疇を超える場合に関しては、当分の間、見解・実行が収斂する可能性は低い。これまで、ロシア・ジョージア（2008 年 8 月）、ロシア・ウクライナ（2014 年、2022 年 2 月～）等、武力紛争に関連するサイバー攻撃事案が国際的に注目されてきたにもかかわらず、実際に各国が国際人道法違反を認定した事例が確認されていないことにかんがみれば、今後も、越境サイバー侵害行動のみで国際人道法が適用される事例は極めて稀とみられる。

Ⅲ　二次的規範及び対処方法

1　各国の立場表明

越境サイバー侵害行動に対して適用される実定国際法の二次的規範、さらに、被害国その他の関係国がどのように対処することが国際法上認められるかについて、Ⅱ 1 と同様の方法で各国の立場・認識を分析すると、行為の国家への帰属及び国家責任の実施に関する規則を含む国家責任法全般が越境サイバー侵害行動についても適用されることについては、中国、ロシアが実際の適用に慎重な姿勢を示しているものの、広範な諸国がその適用を肯定し、又は適用がある前提で立場を表明している。

紛争の平和的解決及び報復については、既に広範な諸国間で越境サイバー侵害行動について適用され得る対処方法として受け入れられている。

対抗措置に関しては、多くの国々が国際法に違反する越境サイバー侵害行動に対して適用され得るとの見解を表明している一方、そのうち一部は、対抗措置の前に責任の履行の要請、対抗措置をとる旨の通告及び交渉の提案を行うとの手続上の要件について、慣習国際法上の義務としての性格に異論ないし疑義を示している。また、中国、ブラジル、ロシアは、対抗措置全般の合法性への疑義（広範な国家実行及び法的確信の有無）、濫用・エスカレーションの危険性、違法な武力の行使に至るリスク等を強調し、越境サイバー侵害行動への対抗措置の適用について消極的見解を示すか、更なる議論の必要性を指摘している。

自衛権に関しては、中国、キューバ等少数の国々がサイバー戦争の適法化を認めるべきでないとの観点から慎重に取り扱うべき旨主張しているものの、広範な諸国の間で越境サイバー侵害行動が自衛権の行使の対象となり得るとの認識が共有されている。

他の違法性阻却事由のうち、越境サイバー侵害行動について緊急状態を援用し得るとする国々が散見されるほか、わずかながら遭難に言及する国も見られる。

2　国家実行又は後に生じた慣行

これまで、越境サイバー侵害行動について、国家責任の実施、紛争の平和的手段による解決及び自衛権の行使のいずれも、実際に行われた事例は確認されない。

行為の国家への帰属に関しては、越境サイバー侵害行動が他国又は他国に所在する個人・団体に帰属することを政府の公式声明、国内刑事手続等により認定した事例は多いが、その行動が国際法違反であることを明示した事例はない。こうした事例のうち、他国への帰属の認定に関しては、越境サイバー侵害の技術的解析（Sony Pictures Entertainment 事案）に加えインテリジェンス情報に依拠したと思われるケース（WannaCry 事案、NotPetya 事案）が見られる一方、他国に所在する個人・団体への帰属の認定に関しては、証拠を以て実行者を特定し、かつ、その実行者及びその

所属する団体が他国の国家機関に属し、又は他国の指導・指揮等の下で活動していることを立証するに至っている場合（Sony Pictures Entertainment 事案、WannaCry 事案、NotPetya 事案）が少なくない。また、前者の他国への帰属の認定は、その根拠となる情報・証拠等の公表を伴わない場合（WannaCry 事案、NotPetya 事案）がある一方、後者の個人・団体への帰属の認定に際しては、起訴状、捜査機関の報道資料等の形で認定の理由、根拠となった情報・証拠等が公表されている。前者が迅速性及び政治的メッセージングにおいて勝るのに対し、後者の「国内司法手続を通じた事実上の帰属の認定」とも形容し得る手法は、帰属の認定過程を非政治化しつつ、越境サイバー侵害行動の実行者と他国との関係まで立証し、その立証の根拠を対外的に公表することができる点に長所がある。

越境サイバー侵害行動への具体的な対応に関しては、国内法に基づく個人・団体への制裁措置、駐在外交官の国外退去等、それ自体は国際法に違反しない、報復に該当する措置がとられたケースがほとんどで、対抗措置がとられた事例は確認されない。また、緊急状態等、対抗措置以外の違法性阻却事由を援用した事例も確認されない。

その一方で、他国からの先行する越境サイバー侵害行動に対する非公然の対応として、被侵害国が大規模な DDoS 攻撃、マルウェアの拡散等のいわゆる攻勢的サイバー防衛措置をとった事例が少なからずあると見られる。例えば、米国が Sony Pictures Entertainment 社事案への北朝鮮の関与を認定した直後、北朝鮮で発生した大規模な DDoS 攻撃によるインターネット接続の遮断（2014 年 12 月）や、2020 年以降のイスラエル・イラン間における給水・運輸・エネルギー・医療の重要インフラを標的としたサイバー攻撃の応酬に関しては、仮に関係国政府の指示・指揮等の下行われたのであれば、相手国の領域主権の侵害が問題となり得たであろう。いずれの例も、相手国の先行する越境サイバー侵害行動への対応として行う場合には本来、対抗措置の援用が検討されて然るべきものであったと考えられるが、関係国が対応に当たり対抗措置の諸要件に縛られることを望まなかったか、イスラエル及びイランについては、越境サイバー侵害行動の相手国への帰属を認定・立証することが困難であった可能性が推察される。

3　考察

行為の国家への帰属に関しては、従来の「指示又は指揮若しくは統制」の判断基準について各国間に異論は見られず、これに代えてＩＣＴＹのタディッチ事件控訴部判決で示された「総体的統制（overall control）」の基準を導入する等により柔軟に国家への帰属を認められるようにすることについて、広範な諸国の支持が集まる見込みは低い。

国家責任の実施及び紛争の平和的解決に関しては、越境サイバー侵害行動への対処に求められる迅速性にかんがみれば、現状では、これらの方法による対処は現実的でない。もっとも、先述の、他国の国家機関に属し、又は他国の指導・指揮等の下で活動する個人・団体に越境サイバー侵害行動が帰属することを国内刑事手続等により認定する手法は、事実関係の認定・立証及びその公表等の面で、国際法上の国家責任の援用・実施においても依拠することができる可能性が高い。今後、米国以外の各国でも国内立法により同様の手法が広まっていく場合には、原状回復や賠償は現実的でないにせよ、侵害国による再発防止の約束・保証や満足を追求する余地を残す上で有益な選択肢となり得よう。

報復に関しては、引き続き、広範な諸国に最も選好される対処方法になると考えられる。

対抗措置に関しては、可逆性、比例性、侵害国に対する事前通告（侵害行為の停止要求・責任の

履行方法・対抗措置の予告・交渉の提案）等の要件を満たすことは必ずしも容易ではないが、武力攻撃に至らない越境サイバー侵害行動に対する最も迅速な対処方法であり、可逆性、侵害国への事前通告の各要件には、一定の例外が認められている。また、そもそも、これを援用する国が侵害国の行為の違法性に関する自らの一方的な評価に基づき、その評価が誤っていた場合には自らの違法な行為について責任を負うこととなるリスクを引き受けてとる措置であり、過去の国際判例においても、そのような性格の措置として慣習国際法上認められていることを確認している。以上にかんがみると、今後、高度の経済的・技術的能力を有する主要国は、大規模かつ重大な損害を伴う越境サイバー侵害行動を受ける場合等には、中国・ブラジル等の異議・批判等ある程度のリスクを負ってでも、対抗措置を援用する可能性があろう。

自衛権の関連では、武力攻撃に至らない違法な武力の行使に対し武力の行使により反撃することは、国連憲章第 2 条第 4 項との関係を始め論争の余地が多々あり、学説上提唱される「比例性を有する対抗措置」、「武力復仇」等によって確実に正当化できるとは言い難い。このため、他国による越境サイバー侵害行動を違法な武力の行使と認定する場合、類似の越境サイバー侵害行動による反撃はそれ自体が違法な武力の行使とされるリスクがあり、事実上不可能となる可能性が高い。したがって、今後、大規模かつ重大な損害を伴う越境サイバー侵害行動に直面する諸国は、武力攻撃と認定し得る例外的な場合を除き、あえて違法な武力の行使とは認定せず、他の一次的規範の違反に基づく対抗措置による対応を選好することが想定される。

他の違法性阻却自由のうち、緊急状態に関しては、越境サイバー侵害行動の他国への帰属及び国際法上の義務違反の認定・立証を要しない、侵害国以外の第三国に影響が及ぶ場合における当該第三国との関係においても違法性が阻却されるという利点があるが、その濫用は攻勢的サイバー防衛の応酬の一般化に繋がるおそれがあり、第三国等から物的損失の補償を請求される可能性があることから、各国は、その援用を慎重に検討するとみられる。

Ⅳ　結論

これまでの学説及び諸国間の議論・実行の蓄積を検証していくと、中・長期的には、大規模かつ重大な損害、特に重要インフラ又は国の公的機関の物理的損壊又は機能の喪失を伴う越境サイバー侵害行動について、被害国の国内管轄事項への違法な干渉又は主権の侵害を成す行為としてその行為の実行地国（領域国）の相当の注意義務違反を認定し、これに対して対抗措置、又は烈度・損害・急迫度が特に多大である場合には緊急避難を援用して迅速に対処しようという規範認識が結晶化しつつあることが看取される。かかる規範認識が広範な諸国に共有され、定着していくに伴い、これに即した国家実行の事例も徐々に現れ、蓄積し、越境サイバー侵害行動に適用される実定国際法規範の具体的内容・判断基準の一層の精緻化に繋がっていくことが期待される。

越境サイバー侵害行動の実行者が、こうした国際法による規律が及ぶことを回避すべく、不干渉義務違反や主権侵害の閾値を超えない低烈度の侵害行動を志向する可能性は排除されないが、仮に現実に国際法で規律・対処すべき大規模・重大な越境サイバー侵害行動の減少に繋がっていくのであれば、具体的な援用・適用の事例がないとしても、実定国際法規範がその実効性を示すものと評価し得よう。