

海底ケーブルの海洋管轄権
—サイバー空間における防御機能の追求—

神田 英宣

海底ケーブルの海洋管轄権

—サイバー空間における防御機能の追求—

神田 英宣

はじめに

海底ケーブル (submarine cables) ¹ は情報通信の中継として海底に存在するが、日常生活では意識されることはまずない。1850年8月、イギリスがドーバー港からグリ・ネ (Gris-Nez) 岬の間に電信ケーブルを敷設して、フランスに送信したのが発祥である²。技術革新によって1990年代、海底ケーブルの電線が同軸ケーブルから光ファイバーに換装されて、インターネット通信が増大した。それは、様々なサービスやコミュニティなどが形成される一つの新たな社会領域、いわゆるサイバー空間となっており、データ通信や音声通話などの国際通信にとって不可欠となった。インターネットが国際的に普及する中で、サイバー空間の持つ重要性や価値への認識が高まっている。今や国際通信量の約95%は、海底ケーブルを伝わって世界の大陸間を行き交っている。そのため、海底ケーブルは重要インフラ (critical infrastructure) ³ に位置づけられている。

サイバー脅威は直接的な人的被害を与えるものではない。したがって、情報データやコンピュータネットワークの防御といったサイバーセキュリティ⁴に焦点が当てられている。これが、組織内の情報保全といった情報セキュリティ⁵の範疇として扱われることもある。またサイバー空間の統治 (ガバナンス) の在り方と国際秩序に関して、様々な国際機関や国際会合で議論が繰り広げられている。その反面、インターネットを構成するシステムとして、海底ケーブルに係る安全保障問題が議論されることは極めて少ない。しかし東日本大震災時、太平洋側の海底ケーブルが切断するなど、緊急事態に情報通信に影響が出たこ

とは事実である。日本が海底ケーブルを活用して100年有余が過ぎるが、その問題意識は海底からなかなか浮かび上がってこない。

エール大学のタラ（Tara Davenport）は、海底ケーブルの保護に関する国際法を整理して、直接的な危害、情報ネットワークの侵害および傍受（monitor）に対する実効性の限界を示している⁶。またユトレヒト大学のユーリ（Youri Van Logchem）は紛争海域を横断する海底ケーブルの管轄権をめぐる、その修理などに従事する第三国の権限が不明であることを指摘している⁷。いずれの論稿も、海底ケーブルに係る国際法の不備を指摘しているが、そのサイバー空間について言及していない。そこで本研究は海底ケーブルを伝わるサイバー空間に着目する。まず海底ケーブルの脅威の推移を辿りながら、その安全保障上の位置づけを明確にする。次に具体的な海底ケーブル保護政策をめぐる法執行を通して、その限界を考察する。最後に、海底ケーブルのサイバーセキュリティを考慮に入れた課題に対して、官民融合のガバナンス機能から解決の道筋を示唆する。

1 海底ケーブルに対する脅威の拡大—インターネットの普及

（1）従来脅威の影響拡大

海底ケーブルはもともと銅線をコーティングした回線であったことから、外的損傷に脆かった。戦時を除けば、その通信遮断の原因は、主として漁業の揚網又は船舶の投揚錨などによるケーブル損傷であった。またその信号通信はスピードも遅く、傍受することも可能であり、通信手段の信頼性も低かった。ところがインターネットの普及により、国際通信が衛星から海底ケーブルに依存するようになると、従来の自然災害によっても、海底ケーブル損傷が国家の経済、国民生活に影響を及ぼしかねないものとなった。2017年、世界中で約428本の海底ケーブルが110万km以上に延びており、大陸間にデータを伝送している⁸。沿岸では水深150m以浅の海域にあり、海底1~3mの深さに埋設されて

いる。それ以外、海底ケーブルは場所に応じて、着底している。このため毎年100～150本の海底ケーブルが障害を受けているが、その原因は今も昔もさほど変わらない⁹。しかしその影響は時には世界経済を揺るがしている。

例えば台湾南西沖地震（2006年）は、ルソン海峡を襲い、日本、香港、シンガポール、マレーシア、そして韓国の経済網を混乱させた。特に韓国では金融経済が機能不能となった。その原因として深度約2,000～3,000m下で、地震直後に震源付近で発生した泥流が付近の海底谷に沿って流れ、海底ケーブルが破断されたものと分析されている¹⁰。その復旧は国際的な敷設支援を得ても2か月以上を要した。また2002年、2003年にも台湾東方沖で海底ケーブル故障が発生しているが、これらの原因は泥流であったとされている。自然災害による通信遮断は予期できないリスクを伴っている。海底ケーブルの損傷を回避するためには、海底谷を回避した敷設迂回路をとる必要があるが、コスト増加を招くことから敬遠されている。他方英国は、30本以上の光ファイバーケーブルをヨーロッパ本土と米国に接続している。これにより漁業活動によって数本が障害を受けても、中断を引き起こすことなくデータをルーティング（経路制御）できるという。

日本はどうだろうか。2006年12月、台湾南西沖の地震により、日本と東南アジアの通信に障害が発生し、復旧するまでに約1か月を要した。しかも海底ケーブルの修理は終わらず、ルーティングによる仮復旧にすぎなかった。また東日本大震災時、日米間および日アジア間を結ぶ海底ケーブルが一部破損して、ルーティングによる応急対策が行われた¹¹。特に日米間の海底ケーブルのほとんどが震源地の海底を伝わっており、完全に復旧したのは同年8月であった¹²。海底ケーブルが被災した場合、日本の海底通信に影響を及ぼすことは避けられない。

（2）新たな脅威

2008年12月、エジプト沖において潜水夫がケーブルを切断した事件は、経済活動や軍事活動に跨って深刻な影響を与え、中東・アジア間の国際情報通信

の約75%に支障をきたした¹³。エジプトは、情報通信の約80%が使用できなくなり、米国は作戦地域の無人航空機（UAV）の運用に支障をきたした。UAVの対テロ作戦データは海底ケーブルを介して前線基地および本国を横断するが、多くの情報ネットワークによって支えられている。そのため、バラード空軍基地（イラク）の飛行回数は極度に減少したと報告されている¹⁴。海底ケーブル通信は完全なバックアップ機能を持ち合わせず、脆弱性を克服できなかった。その通信維持は、海底ケーブルのルーティングにより凌いだのである。そのような脆弱性は安全保障上の懸念を生む。台湾海峡で紛争が発生した場合、海底ケーブルは中国の軍事目標になると警告されている¹⁵。意図的に海底ケーブルがターゲットにされたならば、国際的な経済活動が混乱して、日本のほかシンガポール、インドネシア、オーストラリアなど、アジア太平洋諸国は深刻な混乱を招きかねない。

また海底ケーブルの傍受活動がなくなっているわけでもない。1970年代、米海軍はオホーツク海に配置されたソ連軍の海底ケーブルを傍受する「アイヴィー・ベル作戦（Ivy Bell Operation）」¹⁶を実施していた。米国はこの作戦で非常に重要な情報を入手していたことから、海底ケーブルの通信傍受や妨害、そして通信内容の改ざんを行ったと推測できる。米海軍が、記録用テープを内蔵した専用傍受器を仕掛けて、ケーブルから漏れ出す微弱な電磁波を記録して解析したとされている。ところが今や海底ケーブルは、光ファイバーに換装されており、その傍受には高度な技術力が必要である。しかしそれを凌駕する技術が発達していることが報告されている。2013年英政府通信本部（GCHQ）が、大西洋の海底に敷設された海底ケーブル（SEA-ME-WE-3）¹⁷に傍受装置を取り付け、そこで交わされる通信情報を収集していたことが暴露された¹⁸。しかもこの通信傍受作戦「テンポラ（Tempora）」には、シンガポールおよびオーストラリアも関与していたと言われている。実際このケーブルは、シンガポールからオーストラリア西部のパース（Perth）に枝分かれしている。オーストラリア防衛信号局（ASD）は、2000年頃からシンガポール国防省の協力を得た上で海底ケーブルにコネク特し、国際電話やネット通信に関する情報を集め

ていたという¹⁹。つまり民間用および軍事用の海底ケーブルの区別なく、テンポラは実施されたのである。

2 海底ケーブルに係る法体系と実効

(1) 海底ケーブルに係る国際法と海洋利用

海底ケーブルの普及によって、1880年代には漁業、投錨などによる損壊や故意の切断などが問題となってきた。このため1884年3月、海底電信線保護万国連合条約（Convention for the Protection of Submarine Telegraph Cables、以下「パリ条約」という。）が署名され、4年後に施行された。ほとんどの主要国がこの条約を締結していたことから、国際慣習法として定着していった。その中でも、この条約で規定された海底ケーブルの損壊に対する処罰など（3項目）は、公海条約（Convention on the High Seas）および国連海洋法条約（UNCLOS）に継承されている²⁰。パリ条約の規定によれば、12海里以遠に敷設された海底電信線の敷設は自由であるが、その損壊については旗国の刑事・民事の責任と注意義務に基づくものとしている。特に海底ケーブルを防護する規定は、敷設海域付近の海上活動を規制したものにはすぎない²¹。

そしてUNCLOSに係る海底ケーブルの規定は、パリ条約および公海条約を尊重しつつ、海洋の自由にに基づくものになっている。まず沿岸国は、領海内で無害通航に係る規制を施すことができるが、その法令は適当に公表されるものとなっている（第21条1項(c)、3項）。その上で、海底ケーブルを領海内に敷設するために、沿岸国の法制度に基づき、沿岸国政府との調整や許認可が必要となる。もちろん、第三国による海底ケーブルに対する無許可による「調査活動」は無害通航に抵触する（第19条2項(j)）。

しかしUNCLOSは、施設（installations）および構築物（structures）の安全水域（safety zones）²²のように、運用上の安全を海底ケーブルに配分していない。領海以遠に、特別な海底ケーブルの保護海域は考慮されていないと解

積できる。ただし、各国の領海と内水以外の領域については、原則としてすべての国が自由かつ平等に種々の目的のために使用する権利が与えられている（公海条約第2条及びUNCLOS第87条1(c)）。その上でUNCLOSは、すべての国がEEZにおいて、海底ケーブルの敷設の自由、海洋の利用（海底ケーブルの運用に係る海洋の利用等）の自由を享有する（第58条1項の一部）ことを明記している。

留意すべき点は領海、EEZ（およびその縁辺部）の海底下の大陸棚の規定が別に示されていることである。まずインドネシア、フィリピンおよびバプアニューギニアといった群島国は、敷設の自由度に若干の制限を加えることができる。UNCLOS第51条2項には、「群島国は、・・・海底ケーブルの位置及び修理又は交換の意図についての適当な通報を受領した場合には、その海底ケーブルの維持及び交換を許可する」と規定されている。基本的にすべての国は、この条の規定に従って大陸棚に海底ケーブルを敷設する権利を有する（第79条1項）ことから、「海洋の自由」が尊重されている。だが「適当な通報」をめぐる許可の要否によっては、沿岸国と敷設国の主張が対立しかねないことになる。したがって群島国は、敷設国の自由をどこまで許容するかという課題を背負っている。

すべての沿岸国は、大陸棚における海底ケーブル又は海底パイプラインの敷設又は維持を妨げることができないが、大陸棚の探査、その天然資源の開発並びに海底パイプラインからの汚染の防止、軽減及び規制のために適当な措置をとる権利が確保されている（第79条2項）。また、人工島開発などの管轄権の不可侵（同条4項）、既存の敷設ケーブルの考慮（同条5項）は敷設国に課せられている。ところが、大陸棚に敷設される海底ケーブルの経路については、海底パイプラインの場合と異なり、沿岸国の同意は規定されていない。

この海洋空間の規定は今日どのような実行を伴うのか。統合的沿岸域・海洋管理の枠組みの中で、沿岸国は海底ケーブルの埋設・修理による環境への影響の軽減や、脆弱な生態系の保護も考慮しなければならない。すでに、海底ケーブルによる騒音、電波放射、熱放射などの影響が指摘されているからである²³。

いわばEEZや大陸棚に係る排他的権利の保護を理由として、沿岸国は領海外における海底ケーブルをめぐる海洋環境の保護に配慮が求められる。

もちろんEEZには、漁業、海洋調査、軍事活動などが交錯する。その中で、海底ケーブルの整備に従事する修理船の活動は、沿岸国の漁業活動のアクセスを制限する可能性がある。また他国の軍事活動が訓練であったとしても、沿岸国が修理海域およびその上空に安全制限を加える場合も考えられる。さらに大陸棚において、修理に従事する他国が沿岸国の海底資源へのアクセスを侵す可能性もある。つまり、海底ケーブルに関わる修理活動には、沿岸国との調整を経た許可が必要となるのである。UNCLOSには、海底ケーブルの維持に関する規定がないため、他国沿岸に到達する海底ケーブル障害に対する修理活動の許可は任意となる。そのため、ケーブルが到達する沿岸国の認可レベルは個々に変わってくる。例えば、中国、台湾およびインドネシアの修理許可は、約1週間以上を要している²⁴。修理国が敷設・修理の遅延を被って、運用上の支障が及ぶ可能性は否定できない。

また、海底ケーブル敷設、維持整備のためには、先行して経路などの調査が必要となるため、沿岸国がそのような自国EEZ・大陸棚内で行う他国の活動を「海洋科学調査」と見なすならば、事前の同意を求めることが考えられる。ただ沿岸国のEEZに延びる海底ケーブルの部分に対して、暗に第三国が情報収集に値する活動をしていても、確証を得ることは難しい。その場合、沿岸国の義務（UNCLOS第56条2項）として管轄権を行使することはできない。また公海における海底ケーブルの敷設も自由であり、一国の軍隊は、この権利に従って軍事目的のために情報収集用の海底ケーブルを敷設することが自由である。他方それに対する情報収集も、航行の自由を行使する合法的作用である。「公海の自由」の趣旨に基づけば、海底ケーブルに対する情報収集活動は否定されているわけではない。

そこで、サイバーセキュリティの観点から海底ケーブルに対する情報収集活動を考察する。軍事攻撃によってケーブルを切断した例は記録にないが、アイヴィー・ベル作戦などの傍受活動は脅威である。それによって得られた情報は、

政治的にも軍事的にも利用されるからである。しかしながら、その活動の性質上、安全保障の脅威として議論されることはない。テンポラは、アイヴィー・ベル作戦と対象が異なっており、グローバル・コモンズとして世界が共有する空間を情報収集した活動である。その海上の傍受活動は、軍事用海底ケーブルだけを対象にしていたとは言い切れない。なぜなら軍も民間海底ケーブルを併用しているからである。しかも、艦船や潜水艦の傍受活動は秘密のベールに覆われ、その対象を把握することは困難である。

アメリカ海軍の原子力潜水艦アナポリス（USS Annapolis）が、「コンピュータネットワーク搾取（computer network exploitations）」という傍聴作戦を実行しているとの報道がある。光ファイバーケーブルで交信されるデータを傍受するには、2つのタッピング（tapping）方法があるようである²⁵。米海軍は将来的に潜水艦から射出する水中無人機（UUV）に傍受活動を担わせる構想を描いていることから²⁶、少なくとも軍事用海底ケーブルの位置確認や類別に供する情報収集は含まれているだろう。実際の方法は機密に伏されており知る由もないが、通信障害が起きれば当事国を類推できても特定することは難しい。UNCLOSは沿岸国に対して、その管轄権に服する者がEEZ、大陸棚のみならず、公海において人為的なケーブル損壊をした場合の処罰法制を整備することを求めている（第113-115条）。ただし、沿岸国の法執行はあくまでも旗国主義に基づいており、公海上で所有国が他国の損壊に対して管轄権を行使することはできない。

EEZにおける傍受活動は、多くの国が公式の抗議を受けることなく実施している。もちろん、傍受活動に通知制度が付帯されるならば、情報収集力に脆弱性を与える。当然のことながら、傍受活動は本質的に機密であるため、通知機能は働かないのである。したがってタッピング、海底ケーブル位置情報などの情報収集活動に抑止力は利かず、UNCLOSが仲立ちして機能することはない。平時の情報活動に対する規制のためには、より包括的で全体的な法制度が必要なのである。

（２）サイバー空間が内在する海底ケーブルの国際法適用の限界

UNCLOSが採択された1982年以降に、海底ケーブル内の空間を含んだサイバー空間の安全保障問題が顕在化してきた。ところが既存の国連機関が所掌するには余りにも多くの課題が分散している。国連は、国際電気通信連合（International Telecommunication Union: ITU）の所掌事項に、サイバーセキュリティに関する規則を当てはめることはできなかった。

その根源はサイバー空間の帰属（attribution）にある。通信ネットワーク、金融取引システム、発電所といった社会経済に不可欠なインフラは、海底ケーブルのサイバー空間を通じて繋がっており、責任の所掌を特定することが容易でない。2010年になって、ようやく、米国や中露を含む15か国からなる「安全保障におけるICT分野の政府専門家会合（Group of Governmental Experts: GGE）」²⁷が設置されたが、2017年6月に開催された最後の会合で、事実上決裂している²⁸。現状では、サイバーセキュリティを包含する情報セキュリティの合意さえ得られていない。国連はサイバー空間の国際的な規範を作るべく取り組んでいるが、海底ケーブルに及ぶものではない。

ここで海底ケーブルのサイバー空間の法的論点を明らかにする。まずグローバル・コモンズとしてのサイバー空間は人工的領域であり、陸域、海域、空域および宇宙に跨がり、その大部分は民間セクターに広がっている。つまりサイバー空間は民間のインフラや情報機器の集合体として存在すると同時に、サイバー空間自体が社会インフラや生活の基盤となっているのである。よってサイバー空間では、攻撃の発信源を特定しにくい上に、コンピュータシステムの攻撃優位により、懲罰的な抑止メカニズムが機能しにくい。したがって国家又は非国家主体（テロ集団など）が、主として陸域から海底ケーブルに内在するサイバー空間を経由させて攻撃を仕掛けることが容易である。また一か所に向けた脅威は波状的に拡散するリスクを高めている。

サイバー攻撃²⁹に対する法的な適用は、タリン・マニュアル（Tallinn Manual）が参考になり得る。タリン・マニュアルはNATOにオーソライズされていないが、サイバー戦争あるいはサイバーセキュリティに関する基準書と

して、NATOサイバー防衛センター（Cooperative Cyber Defence Centre of Excellence: CCD COE）が策定したものである。2016年2月、その初版がタリン・マニュアル2.0に更新されている³⁰。この内容は、平時から有事に至る、サイバー空間の武力攻撃に関連する国際法の適用解釈である。

CCD COEは、直接的に死者、負傷者、重大な破壊行為を引き起こすサイバー攻撃は武力行使と見なしており、自衛権行使（国連憲章第51条）の対象にしている。その防御対象は、サイバー空間を創り出す情報システムおよびネットワークとその構成要素（特にコンピュータ）³¹であって、海底ケーブルを含むものかどうかは明らかにしていない。今のところ、沿岸国の領海内において潜水艦やUUVが、タッピングにより海底ケーブルを傍受する活動でさえ、主権侵害の是非をめぐって意見の一致を見ない。海域を問わず、海底ケーブルの障害を引き起こすタッピングは、意図的でないにせよ沿岸国および敷設国に対する損壊（UNCLOS第113条）に値する意見が主流である³²。しかし、現行の国際法を海底ケーブルのサイバー空間に適用できるか否かは不透明である。

ではサイバー攻撃対処のために、海底ケーブル本体を防御することはどこまで許容されるのか。タリン・マニュアル2.0は、開戦条件の規制（*jus ad bellum*）と武力行使手段の規制（*jus in bello*）という2つの課題を基本としている³³。まず国連憲章第41条（非軍事的措置）及び第42条（軍事的措置）の原則は、サイバー攻撃対処のために、重要インフラの保護に効果的に機能するとは考えにくい。第一に、帰属の問題である。国際法は、非国家主体が意図的な障害を与えることを想定していない。仮にサイバー犯罪条約を根拠にして攻撃の帰属が特定できても、攻撃主体を断定できるとは限らないのである。第二に、意図的なネットワーク脅威がサイバー空間の障害を引き起こしたとしても、海底ケーブル本体への物理的危害を伴うとは限らない。第三に、比例適合性原則（*principles of necessity and proportionality*）である。海底ケーブル内を伝わるサイバー空間の攻撃に対して、相応する対処が求められる。だがこの原則をサイバー空間に当てはめることは、被害度を厳密に認知できない限り不可能である。たとえ国家がサイバー空間を構成する海底ケーブルを特定したとしても、

その対応が制約される、あるいは過剰になるばかりか、第三国への攻撃になり得ることもあろう。以上の3点から、海底ケーブルに内在するサイバー空間そのものに適用することは困難である。

またタリン・マニュアル2.0は、海底ケーブル本体の主権については、そのコンソーシアム運営を理由として明記していない（規則54第2項）。他方、沿岸陸揚局から沖合の領海までは、沿岸国の主権の及ぶ範囲である。もちろん、沿岸国は自国の沿岸にある海底ケーブル施設への攻撃に対応できる。あるいは隠密性の点から稀なケースかもしれないが、情報収集活動に伴った物理的危害に対する対応が考えられる。いずれにせよ自衛権行使として、海底ケーブルに対する物理的攻撃に対処できるかもしれないが、そのサイバー空間に及ぶものではない。

3 海底ケーブルの保護とサイバーセキュリティ

（1）オーストラリアなどの海底ケーブル保護規定

実際に海底ケーブルの規制を立法化している例を取り上げて、その実効性を考察してみたい。最初に海底ケーブル保護制度を確立した国は、オーストラリアである。インターネット普及は、海底ケーブルのサイバー空間に対する重要性を認識させた。オーストラリア周辺海域では、国際通信の約95%が海底ケーブル（約19本）によって交信されている。西オーストラリア海域では、パースからスンダ海峡にかけて、東オーストラリア海域では、シドニー（Sydney）から南太平洋に向けて海底ケーブルが集中して敷設されている³⁴。

2007年1月、オーストラリア通信メディア庁（ACMA）³⁵は、海底ケーブル保護法令に基づきパースおよびシドニーの保護区を設定して、具体的に海上活動を規制している³⁶。オーストラリアの処罰対象は、海底ケーブルの損傷および切断、および障害を与えかねない活動であり、100m以浅に適用される。その処罰は、10年以下の懲役、約10万豪ドル以下の罰金と規定されている。100

m以深から限定的ではあるが活動が緩和され、500 m以深では、海上標識の定期整備、海底鉱物や石油の掘削活動、海上交通に係わる技術的活動、軍事訓練は許可制になっている。もちろん、海岸付近500 m以内のレジャーや上層域の遊漁には規制はなく、海洋利用は許可されている³⁷。シドニーの海底ケーブル保護区から約200km以遠には空軍訓練域³⁸が設定されているが、ケーブル事業者が活動する際は軍との調整が求められており、これは安全上の配慮である。基本的には、海底ケーブルに対して、漁業や浚渫作業などは制限されるが、傍受活動や他国の軍事活動が抑制されるわけでない。

海底ケーブルは損傷や破損の影響を受けやすく、情報交信に深刻な影響を与える可能性がある。ここで、海底ケーブル所有者のみならず、利用者である政府機関、企業および個人に、データの損失、著しい情報遅延および深刻な経済的・安全保障的な損失を引き起こしかねない懸念が生じる。そのためオーストラリアは、ケーブル障害修理の調査、脅威の識別および修理の安全確保のために軍の協力を必要としている³⁹。

他方ニュージーランドもオーストラリアと同様に、海底ケーブル保護区域をオークランド（Auckland）の東西沿岸部および北島・南島を結ぶクック海峡に設定（11区）しており、領海内の活動を制限している⁴⁰。海底ケーブルを損傷した場合、最大25万NZドルの罰金が課せられる⁴¹。警察および海軍は海上法執行権を有し、EEZ（およびその縁辺部）まで監視活動を実施している。

オーストラリアおよびニュージーランドの取り組みは、あくまでも国内に対する規制であり、海底ケーブル本体の保護を図るものである。したがって、領海あるいはEEZの一部に管轄権を設定しているだけであって、サイバー空間の障害については法的規制の枠外にある。しかもこの二国のほかに、具体的な海底ケーブルの施策を見ることはない。その理由の一つとして、海底ケーブルの国際機関が所在しないことである。国際海事機関（IMO）が海底ケーブルの輸送関連の側面に関与するかもしれないが、その実効力は限定的である。IMOは、船舶の安全及び船舶からの海洋汚染の防止等、海事問題に関する国際協力を促進しているのであって、海底ケーブルを担当する国際機関としては

適していない。またITUは、情報通信技術に関する主要な国連機関であるが、主に国際的なラジオ帯域と衛星軌道の割当、ネットワークおよび技術がシームレスに相互に接続できる基準を策定しているため、海洋問題には関与していない。

二つ目の理由は、海底ケーブルの運営形態がコンソーシアム⁴²であることによる。近年の海底ケーブルのほとんどは、欧米をはじめとする他国参入による共同出資によって、敷設・運用・保守が営まれており、各国政府が海底ケーブルに主権を主張できる状況になっていない⁴³。つまり海底ケーブルが重要インフラであるものの、ほとんどの国はそれを取扱う主導機関を有してはいない。よって関連する法規は体系化されず、安全上の政策が取られてはいない。海底ケーブル、ケーブル敷設／修理船に係る法的地位、および海底ケーブルシステム（サイバー空間を含む）の意図的な障害に対する国際的な取り組みが求められている。一方各国のケーブル事業者は、電気通信の標準化、ライセンス供与（陸揚局用）、競争上の問題に焦点を当てており、海事問題に関心は寄せられていない。このため、敷設・修理に係る調整メカニズムとして、経路等の調査活動、緊急時の修理協力などの協定枠組みが定式化していない。ケーブル事業者は適切なルールに従って、透明性ある活動に従事しているわけではないのである。

（２）海底ケーブルの国際ルール形成の課題

海底ケーブルの法的な規制が限定的である中、現実的には様々な脅威によって障害が惹起されている。またそれが安全保障上の問題に直結するかどうかの分別もつかない。最も懸念すべき問題は海底通信が遮断されることである。前述したように、海底ケーブルの侵害に対する安全保障および責任に対する特効薬はない。情報収集活動は法の網目をすり抜け、法規制は働かない。

ファイアウォールの構築やハッカーに対するサイバー防御などは、日々ソフトウェアを更新することによってサイバーセキュリティを向上させている。それはあくまでも一連のコンピュータシステムが正常に稼働していることを条件にしたものである。そのようなサイバーセキュリティの向上は、データへのア

アクセスを長期間失いかねない海底ケーブル損傷には無力である。実際にはすべての国やケーブル事業者が、確固たる安定な運用を保証することはできていない。

海底ケーブルに対する物理的な攻撃の蓋然性は低いものの、海底ケーブルネットワーク管理システムに対するハッキング（hacking）は、情報通信を遮断しかねないサイバー攻撃そのものである。また台湾（2008年）や日本（2011年）の地震時のように、サイバー空間のアクセスが閉ざされたならば、そのすべてのデータへのアクセスが失われる可能性が生じる。しかも海底ケーブルの通信網は、国際的なデジタル通信インフラとして機能し世界中に拡大している。この相互依存関係は、サイバー問題が非常に複雑で解決しにくい理由の一つであり、国家の境界を超えた企業の連携が欠かせない。

では国際通信を防護するにはいかなる対策が効果的なのか。自然や人為的事故による通信遮断から防護するためには、海底通信システムを強化することが求められる。この対策には、海底ケーブルの所在海域を監視することや脅威対処訓練を行うのではなく、情報通信システム全体を組み込んだサイバー空間構成要素の解決策を講じることが適当であることは明らかであろう。一つはデータの重複管理である。データ送受信のアクセスを一つにすることは効率的ではあるが、安全保障の懸念を増幅させる。したがって複数の場所に情報を格納し、そのデータへの複数のアクセスポイントを持つことは、データ管理の上で保存性や回復性の利点を発揮できる。

アリゾナ大学のデリック（Derek Bambauer）教授は、データを複数の場所からアクセスすることによって効率性が生まれ、意図的な攻撃を抑止できると主張する⁴⁴。このような解決は、インターネット施設全体の構築に直結する。そこでサイバーセキュリティを高めるために、ある組織が別々の予備情報を維持することを規定化することが考えられる。もちろんデータがルーティングすることによって復帰するようなシステム構築の技術的進展が伴わなければ、海底ケーブルの脆弱性を補完することはできない。ここで問題となるのが安全保障上の価値を指し示す、バックアップする情報源の範囲や機能回復までの時間

を追求することである。確かにクラウドコンピューティングは⁴⁵、この問題に技術的に解消する手段となる可能性を秘めている。データ侵害の際に被害者が復旧できるようにするバックアップ機能であることから、データへのアクセスが維持できるからである。しかしアマゾン社やグーグル社などによる米国主導のシステムが、ロシア、中国などの情報セキュリティ基準に合うかどうかはわからない。

それではサイバーセキュリティのガバナンスは、伝達手段の主軸である海底ケーブルに機能しないのか。国際ケーブル保護委員会（International Cable Protection Committee: ICPC）⁴⁶は、海底ケーブルを所有し、運用している民間企業によって形成された。当初その民間レジームは、北大西洋地域を対象として、漁網や錨などによる不慮の事故から海底ケーブルを保護することを目指していた⁴⁷。今日 UNCLOS に則って、海底ケーブルの経路計画、敷設、運用、維持および保護に関する諸問題に関する勧告が行われている。それは、他の国連機関などとの協力の上に成り立っている⁴⁸。ただし ICPC の勧告は、あくまでもガイドラインとして提起されたものであり、ケーブル所有者間の合意が優先される。

2010年、オーストラリアを皮切りに、シンガポール、ロシアなどの主管官庁に加えて、米海軍が参加している。これらの政府機関は総会における議決権はないが、ICPCは官民融合のガバナンスとして関係国の政府関係者の意識を高めて、国内法制の整備を醸成している。ICPCの構成は、60か国以上、165以上の企業に拡大している。この官民の共存関係に着目すれば、サイバーセキュリティに関する国際的なルール構築に寄与できるかもしれない。例えば2011年、APEC情報通信ワーキンググループ（APECTEL）は、海底ケーブル情報共有プロジェクト（Submarine Cable Protection Information Sharing Project）をまとめた。その中で、各国が海底ケーブルに関する経済や安全保障の政策を確認している。各国がそれに係る経済的な規制要件や保護対策の立法措置、情報保護システムの開発に向けて情報共有を図る意思が窺える⁴⁹。2012年、第9回閣僚会議において、規制枠組みや先進的な取り組みを共有するほかに、サイ

バーセキュリティや海底ケーブルの保護などに対する認識の向上が確認されたことは⁵⁰、その証左と言えよう。

海底ケーブルは通信施設として扱われるものの、実際にはインターネットを構成する網目の一部である。ICPCは、海底ケーブル陸揚局の安全管理システム構築を勧奨することができる。無防備な陸揚局が安全なソフトウェア使用によって、海底ケーブルをモニターする必要があると言われている⁵¹。ICPCが外部監査機能を働かせ、陸揚局とICPCが共に相互モニターするならば、グローバルにサイバー空間の安全を沿岸国の入り口で強化することができる。このような海底ケーブルの問題解決向上はサイバーセキュリティの一翼であることから、ICPCがサイバーセキュリティに関与を深めるのは自然である。今後ICPCが国連機関、特にGGEとどのように連携を図るのかを注視する必要がある。

おわりに

本論は、海底ケーブルの視点からサイバーセキュリティの課題を導出するにあたり、次のことを明らかにした。第一に、海底ケーブルの脅威が、自然災害や人為的事故だけではなく、テロや傍受活動に拡大していることである。さらに海底ケーブルが増設されていることから、その影響度は計り知れない。第二に、海底ケーブル本体に係る法規制はUNCLOSに網羅されていないばかりが、それに内在するサイバー空間に対する侵害に対して、国際法の適用が非常に限定されることである。この空間の法体系は、海底ケーブル本体と一体化して整理できていないことを意味し、更なる論議が必要である。第三に、海底ケーブルの安全保障上の抑止力は、官民の協力が不可欠であることである。これは海底ケーブルのサイバー空間に着目した防護策には専門的な知識を持った事業者の支援を必要としており、官民融合のICPCの勧告が国家の政策決定に一層影響を与えているからである。国連下のサイバーセキュリティの議論に海底ケーブルが組み込まれることは時間の問題かもしれない。

サイバーセキュリティをめぐる、大国どうしのガバナンス的なアプローチ

が機能しなくなっている。情報通信のフローが増大しているが、透明性や多様性にブレーキがかかっているのである。他方 ICPC は海底ケーブルの国際的規範を作り、これに内在するサイバー問題を共有できるガバナンスである。何より ICPC は企業体を主体としており、実務の実行を伴う。したがって海底ケーブル本体の責任が、ケーブル所有者だけではなく利用国にも負担されるならば、グローバルな安全保障認識が醸成されよう。

注

- 1 海底ケーブルは用途により、概ね次に3つに分類できる。①音声を含む情報通信を交信するケーブル、②パッシブソナーにより音響観測するケーブル、③海洋プラットフォームや風力発電機などの施設 (installations) などに電力を供給するケーブル。③は施設システムの一部として捉えられるため、本稿は①及び②を研究対象とする。
- 2 『英国における海底ケーブル百年史』(国際電信電話株式会社、1971年8月)、13-17頁。日本は大北電信に敷設許可を認可し、1872年1月に長崎・ウラジオストック間、1884年2月に長崎・釜山間に海底ケーブルによる通信が開始した。有山輝雄『情報派遣と帝国日本Ⅰー海底ケーブルと通信社の誕生』(吉川弘文館、2013年6月)、81、142頁。
- 3 例えば、米国やオーストラリアは、情報通信、化学、防衛産業、エネルギー、交通などに分類。Office of the Press Secretary, “Presidential Decision Directive/NSC-63,” U.S. Government, May 22, 1998, p. 1.; Critical Infrastructure Centre, “Critical Infrastructure Resilience Strategy: Policy Statement,” Commonwealth of Australia, 2015, p. 2.
- 4 電子的方式、磁気的方式その他の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、もしくは受信される情報の漏えい、滅失又は毀損の防止その他の情報の安全管理のために必要な措置、ならびに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(被害防止のために必要な措置を含む。。「サイバーセキュリティ基本法」(平成26年法律第104号)第2条のほか、欧米の定義と同意。集団防衛の一部として、サイバー攻撃に対する防衛措置あるいは先制予防措置をいう「サイバー防衛」とは区別する。NATO website<https://www.nato.int/cps/en/natohq/topics_78170.htm> 参照。
- 5 情報セキュリティマネジメントシステム (ISO/IEC 27002) における機密性 (confidentiality)、完全性 (integrity)、可用性 (availability) を示す。本稿では、サイバーセキュリティを包含する。
- 6 Tara Davenport, “Submarine Cables, Cybersecurity and International Law: An International Analysis,” Catholic University Journal of Law & Technology, vol. 24, No. 1, December 2015, pp. 66-109.
- 7 Yuri Van Logchem, “Submarine Telecommunication Cables in Disputed Maritime Areas,” Ocean Development & International Law, August 5, 2013, pp.

- 114-115.
- 8 Alan Mauldin, “Frequently Asked Questions: Submarine Cables 101,” *TeleGeography*, February 14, 2017, <https://blog.telegeography.com/frequently-asked-questions-about-undersea-submarine-cables> (accessed March 8, 2018).
 - 9 Lionel Carter et al. , “Submarine Cables and the Oceans - Connecting the World,” UNEP World Conservation Monitoring Centre, December 2009, p. 45.
 - 10 “Submarine Cables Cut after Taiwan Earthquake in Dec 2006,” *Submarine Networks.com*, March 19, 2011, <https://www.submarinenetworks.com/en/news/cables-cut-after-taiwan-earthquake-2006> (accessed March 8, 2018).
 - 11 「平成23年版 通信情報白書」(総務省、2012年3月)、7頁。
 - 12 NTT ComおよびKDDIは、それぞれ4本、5本の日米間の海底ケーブルを保有するが、紀伊半島から米国を延びる各1本が無傷であった。「日本と世界をつなぐ「情報の生命線」海底ケーブル新時代」(KDDI NEWS、2012年12月)、<https://time-space.kddi.com/special/specialreport/20121208/> (accessed May 5, 2018); 「災害にも強い通信ネットワークとクラウド環境の実現に、全力で取り組む」(ビジネスコミュニケーション、Vol. 48 (No. 10)、<http://www.bcm.co.jp/site/2011/10/ntt-com/1110-ntt-com-01.pdf> (accessed May 5, 2018)。
 - 13 “Third undersea Internet cable cut in Mideast,” *CNN International Edition*, February 1, 2008, <http://edition.cnn.com/2008/WORLD/meast/02/01/internet.outage/> (accessed March 8, 2018).
 - 14 Michael Sechrist, “Cyberspace in Deep Water: Protecting Undersea Communication Cables,” Harvard Kennedy School, March 23, 2010, pp. 9-11.
 - 15 Eli Huang, “China’s cable strategy: exploring global undersea dominance,” Australian Strategic Policy Institute, December 4, 2017, <https://www.aspistrategist.org.au/chinas-cable-strategy-exploring-global-undersea-dominance/> (accessed January 11, 2018).
 - 16 Morris, Caitlin, “Operation Ivy Bells: Lessons learned from an ‘intelligence success’,” *Journal of the Australian Institute of Professional Intelligence Officers* (Vol. 20, No. 3), 2012, pp. 17-29.
 - 17 この海底ケーブルは英国から欧州、インド、中国、日本およびオーストラリアを結んでいる。Ian Allen, “Western spy agencies tapped major undersea fiber optic cable,” *Intelnews.org*, August 29, 2013, <https://intelnews.org/2013/08/29/01-1331/> (accessed March 8, 2018).
 - 18 “GCHQ taps fibre-optic cables for secret access to world’s communications,” *The Guardian*, June 21, 2013, <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> (accessed March 11, 2018).
 - 19 Philip Dorling, “Australian spies in global deal to tap undersea cables,” *Sydney Morning Herald*, August 29, 2013, <https://www.smh.com.au/technology/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html> (accessed March 8, 2018).

- 20 UNCLOS第113条、114条、115条および公海条約第27条、28条、29条は、それぞれパリ条約第2条、4条、7条の内容を包含して、各国の海洋政策に委任。他方、大陸棚条約（Convention on the Continental Shelf）は海洋の自由を尊重し、第4条に海底ケーブルの敷設、維持を規定。
- 21 第5条：ケーブル敷設船は特別灯を灯火するものとし、航行船舶は最低1海里避航。特に敷設作業の通知後24時間、漁船は避航。第6条：航行船舶、漁網および漁具は敷設ブイから0.25海里離隔。第7条：船舶所有者は海底ケーブルを保護するために、錨、網および漁具を犠牲にしたことを証明するならば、ケーブル所有者から補償を授受。
- 22 「国連海洋法条約」第60条5項。
- 23 Karin Meißner et al., “Impacts of submarine cables on the marine environment – A literature review,” Institute of Applied Ecology Ltd, September 2006, pp. 16-76.
- 24 “Submarine Cables and BBNJ,” International Cable Protection Committee, August 1, 2016, pp. 17-18.
- 25 ①海底ケーブルに別のケーブルを接合して信号を分断すること、②海底ケーブルを折り曲げてデータの漏えいするポイントをつくる方法。M. Zafar Iqbal, Habib Fathallah, Nezh Belhadj, “Impacts of submarine cables on the marine environment – A literature review,” IEEE, December 2011, pp. 164-168.
- 26 神田英宣「海洋における軍事活動の無人化－USV・UUVの自律能力の射程」（防衛大学校紀要第115輯、2017年9月）、28頁。
- 27 2010年12月、国連総会第一委員会（国際安全保障と軍縮）が設置、2017年には25カ国に拡大。2011年9月に中露等が連名で、「情報セキュリティのための国際行動規範」（code of conduct）の策定を提案。その内容は情報セキュリティの確保に関して各国の主権の尊重を強調し、①他国の政治、経済、社会的安定性を弱体化させる情報等を阻止するための協力すること、②サイバー空間における権利及び自由は、③関連する国内法令に従う前提で尊重すること等が盛り込まれたもの。
- 28 2015年GGEは、国連のルール策定に向けて意見の一致を見たが、その背景には、欧米諸国が規範策定で主導的な役割を果たしてきたことから、中国やロシアが警戒心を示し、合意に反発したためである。「サイバー空間に対する諸外国の施策動向調査報告書」（内閣サイバーセキュリティセンター、2015年3月）、219頁。
- 29 通信ネットワークにおいて、①侵入して情報を混乱、拒否、劣化又は破壊、②本体内のシステムを破壊する行為、③侵入して情報を搾取。
- 30 北大西洋条約機構（NATO）の研究施設協調的サイバー防衛研究拠点（CCDCOE）において、NATO加盟国の軍人や政府職員、弁護士や研究者などが集まり、サイバー防衛に関する研究が行われている。その研究成果として、2013年、米国海軍大学校教授のマイケル・シュミット（Michael Schmitt）以下の国際法学者（17名）らがTallinn Manual 2.0を更新。
- 31 NATO Cooperative Cyber Defence Centre of Excellence, Tallinn manual 2.0 on the international law applicable to cyber operations, Cambridge University Press, February 2, 2016, p. 417.
- 32 Ibid., pp. 257-258.
- 33 Ibid., p. 3.
- 34 TeleGeography, *Submarine Cable Map* (Washington DC/San Diego/Exeter/Singapore: TeleGeography, 2016),

<http://submarine-cable-map-2016.telegeography.com> (accessed July 5, 2017).

- 35 2005年7月1日に、オーストラリア通信庁 (ACA) 及びオーストラリア放送庁 (ABA) が統合し、通信、放送分野の規制監督機関として設立された。ACMA は、電気通信事業及び放送事業、放送コンテンツの規制・監視ならびに周波数管理を所掌。
- 36 ① 船上から、海底上あるいはその付近や中層域で、底引き網を曳航、運用及び吊下。② 船上から、浚渫機及び採貝機を曳航、運用及び吊下。③ 船上から、延縄及びトロットラインを含む流し網を曳航、運用及び吊下。④ 集積地点及び他の洋上集積地点 (洋上廃棄を含む) を設定、維持及び利用。⑤ 船舶を沈めるか、沈めようとする。⑥ 魚を誘ひ寄せる簡易的機能 (集魚装置を含む) を持った錨泊機を曳航、運用及び吊下。⑦ 底引き網を曳航、運用及び吊下。⑧ 海底に達する漁業やその他規制された活動で使用される網、綱、チェーンなどを曳航、運用及び吊下。Australian Communications and Media Authority, Submarine Cable (Perth Protection Zone) Declaration 2007, September 24, 2007, clause 8.
- 37 Australian Communications and Media Authority, Submarine Cable (Perth Protection Zone) Declaration 2007 Explanatory Statement, p. 9.
- 38 訓練区域 Evans Head Air Weapons Range が陸岸から約 50 m に設定されているが、戦闘機 (F-111) は地上目標に対地射撃を実施。オーストラリア国防省ウェブページ、<http://www.defence.gov.au/AircraftNoise/EvansHead/Practice.asp> (accessed March 8, 2018)。
- 39 Rory Medcalf James Brown, “Defence challenges 2035: Securing Australia’s lifelines,” Lowy Institute for International Policy, November 2014, p. 15.
- 40 Annual NZ Notices to Mariners, New Zealand Nautical Almanac 2014 – 15, pp. 253-254.
- 41 Ministry of Transport, Submarine Cables and Pipelines Protection Act 1996, New Zealand, May 16, 1996, clause 11.
- 42 例えば2017年9月、NECはフィリピンと米国本土を結ぶ海底ケーブル「Southeast Asia-United States Cable System」の敷設を完了し、グローバル通信事業者6社に引き渡した。
- 43 土屋大洋「海底ケーブルと通信覇権—電信の大英帝国からインターネットのアメリカへ」『海洋国家としてのアメリカパックス・アメリカナへの道』(千倉書房、2013年10月)、pp. 166-171。
- 44 Derek E. Bambauer, “Conundrum,” Minnesota Law Review, 2011, p. 638.
- 45 インターネットを通じてコンピューターのハードウェアやソフトウェアにリモートでアクセスし利用すること。「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」(経済産業省、2013年)、8頁参照。
- 46 1958年、海底ケーブル所有者と運営者が保護対策の協議を行い、ケーブル損害委員会 (Cable Damage Committee) を設立したが、1967年に自然災害や人為的障害から保護する目的を打ち出し改称。
- 47 設立当初、北海および大西洋に敷設位置を記した海図が漁業者に配布された。さらに国際水路局 (IHB) の協力を得ながら、より実用的な海図がケーブル事業者や水路調査機関に分配された。D. P. F. Chisholm, “The International Cable Committee,” Telecommunication Journal, Vol. 46, 1978, p. 30.
- 48 国連水路機関 (IHO)、国連環境計画 (UNEP)、国際海底機構 (ISA)、国際電気通信連合 (ITU) のほか、シンガポール国際法センター、アメリカ海洋法・政策センター、中国海事協会、国際大電力システム会議と協定。

- 49 APEC Telecommunications and Information Working Group, Submarine Cable Information Sharing Project: Legislative Practices and Points of Conduct, March 2012, p. 5.
- 50 “Building Confidence and Security in the Use of ICT to Promote Economic Growth and Prosperity,” APEC Joint Ministerial Statement, August 7, 2012, clause 6.
- 51 Michael Sechrist, “New Threats, Old Technology Vulnerabilities in Undersea Communications Cable Network Management Systems,” Harvard Kennedy School, February 2012, p. 17.