

海底通信ケーブル防護のための 日本の海洋ストラテジック・コミュニケーション

Japan's Maritime Strategic Communication for Protecting Submarine Cables

矢野 哲也

Tetsuya YANO

大阪経済法科大学 法学部教授

目次

はじめに

I. 日本の海底通信ケーブル防護の現状

II. 海外の海底通信ケーブル防護の現状

III. 海底通信ケーブル防護のための海洋ストラテジック・コミュニケーション

おわりに

キーワード：海底通信ケーブル防護、海洋ストラテジック・コミュニケーション、
映像プロパガンダ戦、YouTube War

はじめに

サイバー戦は、今や海底もその舞台としつつある。2015年10月25日付の『ニューヨーク・タイムズ』紙（電子版）は、ロシアの潜水艦及びスパイ船が地球上のインターネット通信の死命を制する海底通信ケーブルの近くで攻撃的な活動を行っていること、また紛争発生時にロシアが海底通信ケーブルに対する攻撃を計画しているかもしれないとして、米国の軍や情報機関が関心を寄せ始めていると報じた¹。そして同紙は、重要な海底通信ケーブルが敷設されている米海軍基地のあるキューバのグアンタナモ湾に向けて、2隻の自走式深海用潜水艇を搭載したロシアのスパイ船「ヤンター」が、米東海岸を航行する様子を米国のスパイ衛星などが継続監視していたことも明らかにした上で、ロシアのそのような活動がNATOの意思決定を麻痺させる宇宙・サイバー・情報及びハイブリッド戦の一環であるとするファーガソン（Adm. Mark Ferguson）在欧米海軍司令官のコメントを紹介している²。一方、ハーマー（Christopher Harmer）戦争研究所上級海軍アナリストは、海底通信ケーブルの切断がロシアにとり欧州とのビジネスの断絶をもたらしかねないことを踏まえると、真の脅威は海底通信ケーブルからのインターネット情報の盗取にあるとしている³。しかも『ネイビー・タイムズ』紙（電子版）によれば、自律型の無人海底

機器には音紋がなく、アクティブ・ソナーにも反響しないため、その攻撃からケーブルを守ることは極めて難しいとされる⁴。

近年、国際的なインターネット需要の78%がWeb、P2Pやストリーミングで占められ、大陸間のインターネット及び電話回線によるデータの95%以上が海底通信ケーブルによって伝送されている⁵。因みに米連邦準備銀行では1日10兆米ドルの取引が、また多通貨決済システム（CLS）銀行では1日47兆米ドルの取引が、さらに国際銀行間通信協会（SWIFT）ネットワークでは195か国の8,300の金融機関が1日1,500万件のメッセージのやり取りを海底通信ケーブルを介して行っている事実を踏まえるならば、それは世界経済の生命線の役割を果たしているといっても過言ではない⁶。そして、このような現状を踏まえバーネット（Douglas R. Burnett）米海軍退役大佐は、2007年3月のベトナムの海賊によるケーブル略奪事件や2010年6月のフィリピンのテロリスト集団による襲撃事件を例に、海底通信ケーブルやケーブル敷設船はテロの対象になり得ないと考えるのは「世間知らず」と警告した上で、次の3項目にわたる対策を提案している。その第1は、政府内における対応機関の一元化や海軍の役割の再認識であり、特に後者については軍艦の艦長による公海上でのケーブル損壊事件に対する法的権限の行使や米海軍と友好国海軍とによる海底通信ケーブルの安全保障協力の強化、また第2は、軍関係機関が行う海底通信ケーブルの防護を目的とした国際机上演習へのケーブル事業者の参加促進を挙げ、その具体例として2009年3月にオーストラリアが実施した政府、国防軍、ケーブル事業者などによる机上演習（Submarine Communications Cable Desktop Exercise）、米海軍大学が主導した英・加・豪・仏・ニュージーランド・シンガポール海軍とケーブル事業者との連携強化、英国沿岸警備隊とブリティッシュ・テレコムとの自動船舶識別装置（AIS）を使用した机上演習、そして第3に、新たな脅威に対する政府、NGO、国際機関、民間部門による共通利益のためのパートナーシップの構築とした上で、世界の海底通信ケーブル・ネットワークに対する安全保障上の挑戦は現実となり、各国政府と海軍はケーブル事業者とともに効果的な国際協力を実現する必要性を強調している⁷。また、米海軍のマティス（Michael Matis）中佐も、海底ケーブルのルートや敷設網についての国際的な防護体制の欠如が、地球規模の海底ケーブルの弱点と指摘した上で、米海軍第6艦隊司令官と米運輸省国家運輸システム・センターによって立案されたAISから船舶情報を関係国が共有することのできる海洋安全セキュリティ情報システム（MSSIS）による新たな試みを提言している⁸。

翻って、わが国を見るならば、サイバーセキュリティの観点から、ようやく海底通信ケーブルに対する安全保障上の脅威を指摘する声は聞かれるものの、未だに対応策に関する提言は出されていない⁹。そして、「民間企業が保有しているために、海底ケーブルに関わる設備を自衛隊や米軍が24時間防衛することは難しい。」¹⁰というハードパワーの限界を踏まえるならば、今後ソフトパワーによる海底通信ケーブルの防護という新たなアプローチは十分検討に値するものと思われる。以上より本小論は、ソフトパワーによる試みとして米国及びNATOの安全保障政策に位置付けられたストラテジック・コミュニケー

ションの考えを基に、日本の海洋における海底通信ケーブルの防護のあり方について考察するものである。なお本小論の構成は、次項以下においてわが国及び海外の海底通信ケーブルの防護の現状を概観した上で、本論としてわが国の海底通信ケーブルの防護のための海洋ストラテジック・コミュニケーションの具体策の列挙をもって政策提言としたい。

Ⅰ．日本の海底通信ケーブル防護の現状

はじめに海底通信ケーブルの中で、インターネット動画配信を担っている国産の光海底ケーブル（OS/OFSケーブル及びSC300ケーブル）の防護構造について見るならば、光ファイバユニットを防護するための部材として、縦添えされた3分割鉄個片（外径6ミリ内径3ミリ、長さ50キロメートルの金属パイプ）と、その周囲に撚られた14本の鋼線（ピアノ線）をもって、水深1万メートル以上の深海での敷設を可能とし、10トン以上の張力に耐えられる強度を持たせているが、それはあくまでも敷設や引き揚げ修理時に発生する張力に対応するためのものとされている¹¹。そして、それ以外にケーブルを防護する主な手段としては、海底に埋設すること及びそれができない場合は捨砕石、コンクリートマット、半割り鉄管あるいは管路のような外部防護機材を使用したり、岩盤部では岩盤に溝を掘り、ケーブルを落とし込んだ後、コンクリートで埋める方法がとられている¹²。そして、このような海底ケーブルの保守は、世界の海域を分割して行うゾーン保守と特定の地域でケーブル船運航者などが保守用ケーブル船と予備ケーブルを提供して行われるプライベート保守の二通りのやり方で行われている¹³。しかし、「通常ケーブルは浅海域ほど外傷を受け易いため強固な外装保護が行われ、深海にいくにしたがって外傷を受ける危険が少なくなるため軽外装のケーブルが適用される」¹⁴という考えが通信事業者において一般的とされており、深海でのロシアによる脅威が指摘される今日、それはあまりにも現実から乖離した考えといわざるを得ない。また、それと併せて海底通信ケーブルの防護という概念が、漁業活動（トロール漁業、底引網など）、大型船による投錨、海底潮流による摩耗、自然災害（海底地震）への対策を意味し、他国の軍事活動による脅威へのそれが全く顧慮されていないことも問題である¹⁵。

それでは、このような海底通信ケーブルの防護に関して、政府はいかなる取組をおこなっているのだろうか。始めに海洋基本法（平成19年法律第33号、以下「基本法」という。）に基づき、内閣に設置された総理大臣を本部長とする総合海洋政策本部について見るならば、海底通信ケーブルの防護という問題は検討対象にすら挙げられていない。因みに基本法に基づき2008年から5年ごとに策定されてきた海洋基本計画、海洋の状況及び海洋に関して講じた施策を取りまとめた年次報告を見ても、海底通信ケーブルという用語は見受けられない¹⁶。また2001年の米中枢同時多発テロを契機に、米国で考え出された海洋状況把握（Maritime Domain Awareness、MDA）という安全保障政策を参考に、2016年7月に総合海洋政策本部が決定した『我が国の海洋状況把握の能力強

化に向けた取組』を見ても、領海等における外国漁船の違法操業、近隣諸国による海洋権益をめぐる挑発的行為、地球温暖化による気象災害、海域での地震・津波災害、海洋汚染等が脅威とされ、海底通信ケーブルの防護については全く言及されていない¹⁷。なお、MDAとは、関係政府機関の連携を強化して国の防衛、安全、経済、環境に影響を与える可能性のある海洋に関する事象を効果的に把握しようとするものであり、現在では米国、欧州ともに海洋安全保障のみならず、海洋からの様々な人為又は自然の脅威に対応するための情報共有基盤として取組が進められている¹⁸。そして2015年に、総合海洋政策本部事務局、国家安全保障局及び宇宙戦略室主導の関係府省等連絡調整会議が報告した『我が国における海洋状況把握（MDA）について』を見ても、海底通信ケーブルの防護に関する記述はどこにもない¹⁹。また、2016年12月に初めて開催された海上保安体制強化に関する関係閣僚会議においても、出席した海上保安庁長官及び国土交通大臣から尖閣領海警備体制の強化と大規模事案の同時発生に備えた体制整備や、海上法執行能力及び海洋監視・調査能力の強化について発言が行われたものの、海底通信ケーブルの防護についてのそれはない²⁰。このほか、海底通信ケーブルを生命線とするサイバー空間の安全保障を担当する内閣のサイバーセキュリティ戦略本部や日本の海上防衛を任務とする防衛省についても、その結果は総合海洋政策本部等と同様である。2015年9月に閣議決定された『サイバーセキュリティ戦略』及び2017年8月にサイバーセキュリティ戦略本部が決定した年次計画の重要インフラを守る取組に海底通信ケーブルの防護は含まれていない。また、防衛省についても、「新・旧」の防衛大綱及び中期防衛力整備計画の中に当該記述は見当らず、防衛白書に掲載された「防衛省・自衛隊におけるサイバー攻撃対処のための総合的施策（サイバー攻撃対処6本柱）」でも、海底通信ケーブル等の重要インフラの防護という概念は欠落している²¹。

Ⅱ. 海外の海底通信ケーブル防護の現状

海底通信ケーブルの通常の保守管理については、前項でも述べたようにプライベート保守のほかに、世界の海域を分割して行うゾーン保守があり、これは複数のケーブルオーナーがケーブル船ゾーン保守協定を結び、障害発生時に迅速な修理が実施できるよう各ゾーン毎にケーブル保守船と修理要員を待機させている²²。また、これとは別に海底通信ケーブルの保護のための国際的な非営利組織として、1958年に英国で設立された国際ケーブル保護委員会（International Cable Protection Committee, ICPC）があり、海底通信ケーブル事業者、ケーブル船運航会社など世界60か国170以上の会員で構成されている²³。そして、2009年4月に行われた海底通信ケーブルネットワーク・セキュリティに関する講演においてICPCは、世界経済に重大な混乱をもたらすネットワークに対する脅威として、東シナ海での海賊によるケーブル機材の略奪やケーブル敷設作業に対する妨害を取り上げ、関係する各国政府に対し、①海賊対策のための政府間協定の締結、②緊急時の政府対

応窓口の一元化、③ケーブル防護を支援する海軍艦艇の展開、④ケーブル事業者が参加する海軍演習や図上演習の実施、⑤ケーブル防護のための国際法の普及の以上5項目にわたる対策を提唱した²⁴。

一方、海底通信ケーブルの防護に最も熱心な米国について見るならば、2013年2月に政府が発出した『重要インフラの安全保障及びその復旧に関する大統領政策指示 (Presidential Policy Directive/PPD-21)』を挙げることができる。それは、サイバー等の脅威から重要インフラの安全性と復元力を強化するため、横断的な政府機能の改善など3項目にわたる戦略方針と、国土安全保障省、国防総省などの各省庁の役割と責任を明示するとともに、重要インフラの定義として、それを破壊することが安全保障、国民経済などの弱体化につながる米国にとって死活的なシステム等とし、これには海底通信ケーブルも含まれるとされる²⁵。また、これとは別に安全保障の見地から海底通信ケーブルの敷設申請を審査する「チーム・テレコム」が、国土安全保障省の主導の下に国防・国務・司法省、中央情報局、国家安全保障局、国家情報長官室の職員で構成されるとともに、2008年には国土安全保障省、連邦通信委員会 (Federal Communications Commission, FCC)、科学技術政策室が、全米の海底通信ケーブル会社からシステムに関するセキュリティ情報の任意提出を求めている²⁶。なおチーム・テレコムは、法的な裏付けのないアド・ホックな組織として発足したにもかかわらず、その役割はFCCが行っている外国企業からの海底通信ケーブルの敷設に関する許認可業務に対する安全保障上の監視機関及びサイバーセキュリティ上のリスクを局限する政策実行機関としての役割を果たしている²⁷。さらに米国は、2017年2月から国土安全保障省と国家情報長官室が中心となって、「官民分析交流プログラム『海底ケーブル通信に対する脅威』チーム」(The Public-Private Analytic Exchange Program (AEP) "Threats to Undersea Cable Communications" Team) を立ち上げ、半年間以上に及ぶ評価分析の後、海底通信ケーブル防護のための勧告を公表して

表：海底ケーブル脅威区分マトリックス

脅 威	陸上～揚陸部	沿岸部～130ft	沖合130～300ft	大陸棚300～600ft	深海～600ft+
自然脅威					
サ ヌ	低	低	中	中	低
地 震	低	中	中	高	高
地滑り	低	低	低	高	高
火山噴火	高	高	低	高	高
津 波	低	高	中	中	中
事 故					
漁業活動	低	高	中	低	低
拔 錨	低	高	中	低	低
底引網	低	高	低	低	低
不法行為					
サイバー攻撃	高	高	低	低	低
破壊行為	高	高	低	低	低
活動家	高	高	低	低	低
窃 盗	低	高	中	低	低
テロリスト	中	高	中	中	低
国家行為	低	中	高	高	高

(出典：Public-Private Analytic Exchange Program 2017, *Threats to Undersea Cable Communications*, September 28, 2017, pp.7-8.)

いる。その中の脅威区分マトリックス（前頁表）によれば、サメ被害、海底地震、地滑り、津波、火山といった自然の脅威や漁業、投錨、底引き網による偶発的な脅威に比べて、サイバー攻撃、破壊主義、窃盗、活動家、テロリストといった悪意に基づく脅威のほとんど全てが陸上部及び沿岸部の両方において、また同じく国家主体によるそれが沖合部、大陸棚及び深海部の全てにおいて、いずれも高強度とされたことは、これからの米国の海底通信ケーブル防護に対する脅威認識の重点がどこに向けられているのかを示している²⁸。

因みに勧告は、海底通信ケーブルに対するリスクの増大に関して、①テロリスト・ネットワークの巧妙化・国際化により、彼等の虚無的な考え方が海底通信ケーブルの破壊というリスクに目を向けてきていること、②敵対国家によるサイバー攻撃の能力と意志が向上していること、そして③海底ケーブル・システムを妨害することのできる国家主体の能力について政府や企業が関心を寄せ始めているとして、オーストラリア政府が2016年に中国企業Huaweiの不透明な活動をもってソロモン群島との間に海底通信ケーブルを敷設する計画を中止した事例を紹介している²⁹。

また米国以外では、国家インフラ防護センターという専門機関を設けて海底通信ケーブルの防護に取り組む英国や、沿岸防護地帯（Coastal Protection Zones, CPZs）を設定し、ケーブル損傷行為に対する罰金を課しているオーストラリア、ニュージーランドの取組を挙げることができる³⁰。なお英国においては、2017年に保守党の下院議員が公表した海底通信ケーブルの防護に関する政策提言に世論の関心が集まった。それは、ロシアの軍事的脅威を強調した上で、①次期戦略防衛レビューにおける検討、②次期国家リスク・アセスメントにおける検討、③国家インフラ防護センターへの陸揚サイト防護の指示、④オーストラリア型CPZsの導入と地中海・スエズにおけるCPZs設定の促進、⑤ケーブル監視装置の展開、⑥ルソン海峡など世界の海底通信ケーブルの要衝を護るための米欧の連帯の促進、⑦バックアップ・ケーブルシステム等の構成、⑧ケーブル防護のための新たな国際法の締結促進、⑨ケーブル防護のためのNATO海軍演習等の促進といった9項目の具体的施策の実行を政府に求めているのが特徴的である³¹。そして、今まで述べてきた海底通信ケーブルへの脅威と各国の取組を踏まえ、わが国としての新たな取組となる海洋ストラテジック・コミュニケーションについて次節以降において考察していきたい。

Ⅲ. 海底通信ケーブル防護のための海洋ストラテジック・コミュニケーション

1. YouTube War

海底通信ケーブルによって支えられたインターネットは戦争の姿を変えた。インターネット需要の大半を占める動画配信は、2003年のイラク戦争を契機に登場したイスラム系反政府武装勢力によってYouTube Warという新たな映像プロパガンダ戦を生み出した。

ノースカロライナ大学のダウバー（Coli E.Dauber）准教授によれば、アルカイダは米軍との交戦で倒されたゲリラ戦闘員の遺体を、あたかも祈祷の最中に殺害されたかのように偽装し、その動画をインターネットに投稿することで米国の世論に訴え、反戦機運の醸成を目論んでいるとされ、そのメディア部門は常に進化しているとされる³²。因みに、『イラク反政府武装勢力のメディア：映像と思想の戦い』というレポートによれば、彼らは映像作品等を製作する複数のメディア・センターを自ら運営し、インターネット上に開設した複数のウェブサイトにて作品をアップロードするビデオテープ作戦を組織的に展開している事実が明らかにされている³³。つまりラップトップ、インターネット、カメラ機能の付いたセルフォーンなどのソフトウェアが、地球規模の影響を与え得ることに気付いた彼らは、「テロリスト・ジャーナリスト」として世界に情報を発信する能力を手に入れ、今や映像を記録するカメラは彼らの有効な武器と化したとされる³⁴。

このような新たな戦争に直面した米軍は、いかにそれに対処したのであるか。そのための施策の一つが、2005年の基地統廃合政策によって四軍の広報作戦を統合運用する国防メディア局（Defense Media Activity,DMA）の創設である。因みに2016年のDMA年次報告によれば、その任務は米軍兵士とその家族のためのメディアサービスの提供に止まらず、公式のウェブサイトを通じて年間9億1400万人の利用者を獲得するなど国防総省の新たなストラテジック・コミュニケーション政策の担い手となっている³⁵。つまり米軍は、外部の報道機関に依存する従来の戦略から、インターネットを媒体に自ら世界に情報を発信し支持者を直接獲得する新たな戦略を構築しつつあり、この傾向はNATOにおいても採用されている。それを象徴するのが、2014年に創設されたNATOストラテジック・コミュニケーションズ・センター（NATO Strategic Communications Centre of Excellence）であり、NATOのストラテジック・コミュニケーション能力の強化のための教育研究をその主な任務とし、ロシアのウクライナやシリアにおけるソーシャルメディアを駆使したプロパガンダ戦の研究成果をインターネット上に公表している³⁶。

そして米国防総省は、このDMAの中に、イスラム武装勢力の映像プロパガンダ戦に対抗する専門機関として、国防映像マネジメント作戦センター（Defense Imagery Management Operations Center, DIMOC）とその部局である統合コンバットカメラ・センター（Joint Combat Camera Center, JCCC）を設置し、戦場における映像を武器に作戦行動に従事するコンバットカメラ（COMCAM）部隊を運用している³⁷。なおCOMCAMについては、『映像情報に関する国防総省指示（DODI 5040.02）』が統合運用の観点から任務等を規定し、米海軍においては『海軍の映像情報プログラム指針と責任区分に関する海軍作戦部長指示（OPNAVINST 3104.1A）』及び『海軍のCOMCAMプログラム指針、責任区分及び手続に関する海軍作戦部長指示（OPNAVINST 3104.3A）』が細部を定めている。因みにDODI 5040.02 では、映像情報に関する指針においてCOMCAM等による映像情報がストラテジック・コミュニケーションを支援すべきことが、またOPNAVINST 3104.1Aでは、ストラテジック・コミュニケーションが広報、情報作戦などを統合するも

のであり、COMCAM部隊はその目的を達成するために広報や情報作戦と密接に連携すべきことが明記されている³⁸。さらにOPNAVINST 3104.3Aは、映像プロパガンダ戦への対抗策としてのCOMCAMの意義について、次のように述べている。

広報目的のための戦闘記録の使用は、民間のニュースメディアが戦闘地域にいないか、遅れて到着する場合に特に重要である。・・・敵は偏見で仕立て上げたストーリーを入念に図った時間に公開したり、多様なメディア情報を使って映像を改ざんすることを知っている。米軍のCOMCAMの記録がなければ、指揮官や報道隊員は時として、たった数語による敵のプロパガンダや誤情報に対抗する機会を失うのである³⁹。

しかも、OPNAVINST 3104.3Aが全ての海軍の活動に適用される旨を定めていることは、COMCAMが有事平時を問わず、その活動と効果を期待されていることの表れであり、米海軍の広報に対する関心の高さを窺い知ることができる⁴⁰。但し、映像プロパガンダ戦に関し、『海軍省の広報指針と諸規則に関する海軍長官指示（SECNAVINST 5720.44C CH-1）』が、広報の諸原則において「プロパガンダは、国防総省の広報プログラム類にお呼びではない」⁴¹と述べていることには疑問を抱かざるを得ない。確かに、プロパガンダが否定的印象を持たれるのは、それが独裁政治の手段とされた歴史を踏まえると仕方ないであろう。しかしストラテジック・コミュニケーションに詳しいポール（Christopher Paul）博士によれば、2001年版の米統合参謀本部編『軍事用語辞典』に掲載されたプロパガンダの定義に否定的な意味合いはなく、むしろプロパガンダとはストラテジック・コミュニケーションとパブリック・ディプロマシーによる宣伝工作とされ、情報源の信頼度に応じてホワイト、グレー、ブラックに区分されるとして、当時の軍は肯定的に理解していたからである⁴²。歴史を振り返るならば、英国の有名な国際政治学者であるカー（E.H.Carr）が、その著書において世論の力を象徴する言葉として用いたのはプロパガンダであり、また同時代の近衛文麿が第一次世界大戦後のパリ講和会議の所感として、時世が日本に要求する急務としたのもプロパガンダ機関の設置と活用であった⁴³。これらを踏まえるならば、プロパガンダはお呼びではないとする現在の米海軍の考えは、カーや近衛に言わせるならば単なる言葉の遊戯以外の何物でもなく、インターネットの普及によって熾烈化する映像プロパガンダ戦において、米国のストラテジック・コミュニケーションは専守防衛を余儀なくされるであろう。

そして、現場海域の実相を即座に伝達することが容易ではない海洋では、敵対勢力よりもより早く正確な情報を世界に発信し、国際世論の支持を獲得することが映像プロパガンダ戦を勝ち抜く必須条件となることから、米軍のCOMCAMはわが国の海洋ストラテジック・コミュニケーションの有効な手段となり得るに違いない。その参考となる事例が2010年に発生した尖閣諸島中国漁船衝突映像流出事件であり、一個人によってYouTubeに投稿された一本のビデオ映像が瞬く間に全世界に拡散し、それ以前は映像内容を否定する

発言を繰り返してきた中国外交部報道官が、流出事件後は「関係する報道に注意している。中国はいわゆるビデオ問題が中日関係を引続き阻害することがないように希望する。」として、暗にその影響力の大きさを認めざるを得ない発言にトーンダウンするに至ったことは、武器としての映像が国際政治に及ぼす力の大きさを証明したものといっても過言ではない⁴⁴。本論文の冒頭で紹介した米国東海岸でのロシアによる海底通信ケーブルに対する攻撃的活動に類似した状況は、わが国本土と沖縄に所在する在日米軍及び自衛隊の基地を結ぶ海底通信ケーブルが張りめぐらされた東シナ海において明日にも生起し得るかもしれない。そして、今日まで海上で繰り返されてきた尖閣諸島をめぐる日中の駆け引きは、今後は海底を舞台とした新たな段階に移行するに違いない。その時、わが国が自衛隊のCOMCAMによって現場海域における真相を世界に知らせた暁には、国際世論戦の主導権を掌握することができるであろう。

2. 専門機関の設置

2015年に米国東海岸で起きた海底通信ケーブルに対するロシアの軍事的行動が、わが国周辺海域で発生した場合、政府はいかなる対応を考えているのであろうか。そのベースとなるものが領海及び内水（領水）内を潜没航行する外国潜水艦に対する海上警備行動であり、海上自衛隊は、こうした潜水艦に対し、国際法に基づき海面上を航行し、かつその旗を掲げることを要求し、これに応じない場合は、領海外への退去を要求するとともに、潜没航行する外国潜水艦を探知、識別、追尾し、上記の国際法に違反する航行を認めないという意思表示の能力及び浅海域における対処能力を維持・向上させている⁴⁵。しかし、広大な海洋における行動の自由は外国潜水艦の側にあることから、それを予測することは不可能であり、わが国は受動的対応に終始せざるを得ない。このような不利を補うためには、海底通信ケーブルをめぐる外国潜水艦に関する情報収集が不可欠であり、諸外国の海軍や国内外の民間事業者、ICPCとの連携にあたる専門機関の設置は、海上自衛隊にとって急務といえるであろう。

そして、海上自衛隊が専門機関を設置するにあたって、その参考となるのが18年前に創設された米海軍の海底ケーブル防護室（U.S.Naval Seafloor Cable Protection Office, NSCPO）であり、NSCPOは全ての海軍保有ケーブルに関する公的窓口として活動するほか、海底ケーブルに関する米海軍の利益代表として、国内における政府関係機関及び産業界との調整や諸外国との連携協力を行っている⁴⁶。因みに、2006年には防護対象が国防総省が保有する全てのケーブルに拡大されるとともに、ICPCにおける加盟団体として代表を派遣したり、全米ケーブル保護フォーラムを通じて情報共有を図るなど、国内外の民間組織との交流も盛んである⁴⁷。また、これとは別に米海軍は、沿岸・海洋・臨海部にある海軍施設に対するグローバルな支援を任務とする海軍施設エンジニアリング・サービスセンター（Naval Facilities Engineering Service Center）を備え、海底ケーブル施設の保守

管理のほか、ケーブル査察のための無人海底移動装置や海中移動目標の音紋測定装置の開発実験にも力を入れている⁴⁸。このように米海軍は、海底通信ケーブルの防護を独立した作戦分野と考え、そのための組織づくりを推進してきており、かつて第1次世界大戦にドイツ潜水艦の通商破壊作戦に苦しめられた経験から、海上交通路の防護を国土防衛と並ぶ任務と位置付けてきた米英海軍の伝統が、今では海底通信ケーブルの防護に受け継がれているといってもよいであろう⁴⁹。

以上の点を踏まえるならば、日本の海底通信ケーブルの防護を目的とする組織を新たに海上自衛隊に設置する意義は明らかにされたといえるであろう。即ち新たな組織は、対内的には民間の通信事業者や研究機関及び関係省庁（総務省など）との連携協力窓口となって情報共有、図上演習等を担任するとともに、対外的には海底通信ケーブルの防護に取り組んでいる米国、英国、豪州などの海軍機関との連絡調整に当ることになるであろう。そして、更に米海軍のNSCPOのようにICPCの加盟団体となり、海底通信ケーブルの防護のための新たな国際ルールづくりにわが国として積極的に参画していくことができれば、日本の海洋ストラテジック・コミュニケーションの成功例となるに違いない。

3. 関係組織との連携

海底通信ケーブルの防護にあたり、海上自衛隊が連携すべきは、ケーブルの保守管理を行っている国内民間事業者であり、ケーブル敷設船を所有する国際ケーブル・シップ社（2隻、他に1隻建造中で2019年運航開始予定）、NTTワールドエンジニアリングマリナ社（3隻）及びコクサイエンジニアリング社（1隻）の3社が該当する。そして、連携の具体的内容としては、既に諸外国が行っている情報の共有や官民共同の机上演習であり、それを可能とする環境もすでに整えられつつある。その最たるものが、2015年に成立した株式会社海外通信・放送・郵便事業支援機構法（以下「支援機構法」と略）であり、従来、多額の資金を必要とした民間の海底通信ケーブル敷設事業が、新たに支援機構法に基づき政府が株式の1/2以上を保有する同支援機構からの資金提供を受け、政府の支援の下に本格的な海外での事業展開が容易となった⁵⁰。そして、支援機構法第24条第1項に基づき、支援対象事業者及び支援内容を決定するにあたって従うべき基準を定めた総務省告示『支援機構支援基準』には、次の一項が定められている。

（5）政府の関係施策との連携

- ① 効率的・効果的に対象事業の支援を行う観点から、必要に応じて、関係省庁、地方公共団体、政府関係機関、対象事業に関連する官民ファンドその他関係者と相互に連携を図り、守秘義務に留意しつつ、情報交換等に取り組むこと⁵¹

因みに、支援機構の株主には政府の外にKDDIやNTTも名を連ねており⁵²、ケーブル敷

設船を所有する前記3社が、いずれもその関連会社であることからするならば、上記支援基準に基づき、海上自衛隊が民間事業者と連携を図っていくことも可能といえる。むしろ近い将来、民間事業者の側から、それを求めてくるかもしれない。なぜなら、2018年2月に公表された総務省の海外展開戦略によれば、光海底ケーブルシステム分野における主なスケジュール・目標は、当面アジア・太平洋地域での事業受注に向け、支援機構等のファイナンスツールを積極的に活用して、わが国企業を支援するとしながら、中長期的には市場の伸長が期待できる大西洋地域の事業獲得に向けた検討を行うとされているからである⁵³。つまり、わが国のケーブル敷設事業者としては、事業のグローバル化に伴い、海底通信ケーブルに対するロシアの軍事的活動が活発化している米国東海岸を含む大西洋地域において、安全保障上の脅威に直面するリスクは避けられないことから、いやでも米英海軍との協力関係にある海上自衛隊との連携を必要とせざるを得なくなるであろう。そして、民間事業者と海上自衛隊が協力して海底通信ケーブルの防護にあたることは、海上自衛隊にとっても今までにない新たな民軍協力活動（Civil-Military Cooperation, CIMIC）の試みとして、これからの日本の海洋安全保障に必要とされるに違いない。

そして、海底通信ケーブルの防護にあたり、わが国が連携すべきもう一つの組織が、ICPCであり、その活動内容に海底通信ケーブルの法的権利を保護するための規則案の検討が含まれていることは、ロシアなどの潜水艦の軍事的活動に対する国際法による規制という観点から海底通信ケーブルの防護にとって有効な手段となり、その規則案作りに海上自衛隊が関わることであれば、わが国の海洋安全保障にとっても有益といえる。因みに2018年8月6日現在、ICPCに加盟する177団体の国別分布を見るならば、米国（33団体）を筆頭に英国（16団体）、日本（8団体）、中国（7団体）、ドイツ及びシンガポール（各6団体）と続き、英国、オーストラリア、ニュージーランド、シンガポール、マルタは政府機関が、また米国はICPCで唯一、海軍（NSCPO）を政府機関の代表として参加させている⁵⁴。

これに関して、現在のICPCのバーネット法律顧問が、米海軍退役大佐という軍出身者であることは、海底通信ケーブルに対する外国潜水艦の軍事的脅威という新たな課題に直面しているICPCにおいて今後益々発言力が高まっていくに違いない。米国の国土安全保障省と国家情報長官室を中心とする官民合同チームが公表した前掲の『海底ケーブル通信に対する脅威』によれば、現在、世界の海底通信ケーブル市場における主要企業7社のうちの3社に日本の三菱電機、富士通、NECがランクされ、また世界の海洋ケーブル全39システムのうち9システムを日本の企業が供給している現状において、ICPCに海上自衛隊の関係者が参加していないことは、ストラテジック・コミュニケーションの観点から致命的といわざるを得ない⁵⁵。よって項を改め、海底通信ケーブルにも重大な影響を及ぼすサイバー戦に関する最近の法規制の動きを例に、ストラテジック・コミュニケーションの重要性について考えてみたい。

4. 新たな国際ルール作りへの参画

エストニアの首都タリンに創設されたNATOサイバー防衛協力センターは、2013年にサイバー戦に関する95項目の国際法上の規則を定めた『タリン・マニュアル』を公にした。そして海底通信ケーブルに関し、「中立」を規定した第7編の中の規則91（中立のサイバー・インフラの保護）は、その注釈第5項において、中立地帯に設置されたサイバー・インフラが中立違反の状況下にある場合は、保護を受ける権利は失われるとともに、海底ケーブルのような中立のサイバー・インフラが中立地帯の外に設置され、それが適法な軍事目標を構成する場合は攻撃又は捕獲の対象となり得ると規定した⁵⁶。おそらく紛争が生起すれば、敵対国家または敵対勢力は、インターネットを駆使したプロパガンダ戦を展開したり、敵の政経中枢に対する大規模なサイバー攻撃を行い、それを可能ならしめる海底通信ケーブルの一部でも中立地帯の外にある限り、即座に攻撃対象となることは歴史が示すとおりである。そして上記規則91をめぐり、草案作成を担当した国際専門家グループで議論されたのは、交戦区域のサイバー攻撃が、中立地帯に重大な影響を及ぼした場合における中立侵害行為の責任の有無についてであり、中立地帯の外における海底通信ケーブルに対する攻撃については何ら議論されていない⁵⁷。領海や公海の別なく展開した海底通信ケーブルの特性を考えるならば、中立地帯の外におけるケーブルへの攻撃が瞬時に中立地帯のネットワークシステムに重大な影響を及ぼすことが明らかであるにもかかわらず、この点の議論がなされなかったことは問題といえる。

またNATOサイバー防衛協力センターは、2017年に平時のサイバー作戦に適用される154項目の国際法上の規則を定めた『タリン・マニュアル2.0』を策定したが、その中の規則54（海底通信ケーブル）に関し、国際専門家グループで問題となったのが、大陸棚上または排他的経済水域における沿岸国と海底通信ケーブル敷設国との間の司法管轄権についてであり、公海自由の原則により敷設国が適当と考えられるものの、実際の議論ではしばしば意見が沿岸国寄りとなり、その結果合意に至らなかった経緯が、その注釈第9項で明らかにされている⁵⁸。これは、国際専門家グループ内での意見対立が、すなわち国際法の未確定領域における各国の利害対立の表れと見ることができ、裏を返すと国際専門家グループに代表者を出していない国はマニュアル策定作業を傍観する外はない。だからこそ2013年の『タリン・マニュアル』の策定作業に専門家を派遣しなかった中国が、2017年の『タリン・マニュアル2.0』において武漢大学国際法研究所の国際法教授を参加させたのも首肯できる⁵⁹。

以上のことからするならば、一連の『タリン・マニュアル』の策定は、将来のサイバー戦を見据えた主要国の、国際法を手段とするストラテジック・コミュニケーションの好例といえるであろう。試みに2013年の『タリン・マニュアル』の策定に関わった軍関係者は、シュミット（Michael N.Schmitt）米海軍大学教授を筆頭に、編集委員会5名中2名（英空軍退役准将、米海軍大学院教授）、法律専門家グループ9名中5名（カナ

ダ海軍法務将校、オーストラリア軍大佐、オランダ軍士官学校教授、スウェーデン国防大学教授、カナダ軍退役准将)、オブザーバー4名中2名(米サイバー・コマンド空軍大佐、NATO軍司令部要員)、論評委員13名中5名(スウェーデン国防大学博士、英海軍中佐、オーストラリア空軍将校、米海軍中佐、米陸軍士官学校大佐)であり、計32名中15名に上る。また2017年の『タリン・マニュアル2.0』においても、シュミット米海軍大学教授の外、法律専門家グループ17名中3名、起草委員9名中6名、法律論評委員58名中20名の計85名中30名が軍関係者である⁶⁰。これらを見ても、サイバー戦のための新たな国際法の策定に各国の国防機関が並々ならぬ関心を示し、彼らが議論をリードしていったであろうことは想像に難くない。因みにストラテジック・コミュニケーションは、2001年の米中枢同時多発テロを未然に防げなかった米国防総省が開発した軍隊によるソフトパワー戦略の代名詞であり、人間同士のコミュニケーション領域という新たな戦場空間において、いかに主導権を発揮できるかという一点に、その成否がかかっている。この点において、防衛省・海上自衛隊が策定作業に関与する機会を得られなかったことは悔やまれてならないが、今回の策定作業において合意に至らなかった海底通信ケーブルに関する敷設国と沿岸国の司法管轄権の問題などは、これからのわが国にとって重要な安全保障上の課題であることから、機会を見つけて海底通信ケーブルに関する新たな国際ルール作りに参画し、敷設国としてのわが国の考えをそれに反映させることが求められてくるであろう。

おわりに

今日、海底通信ケーブルが国際社会に果たす役割は計り知れず、わが国はその敷設事業において世界有数のシェアを有するにもかかわらず、それが今や国家による不法行為の脅威に曝されている現実についてはほとんど顧みられていない。このような現状に対し、今のわが国に必要とされているのが、海底通信ケーブル防護のための海洋ストラテジック・コミュニケーションであり、そのための具体的な施策として、国際世論戦に備えた自衛隊COMCAM部隊の整備、海上自衛隊における海底通信ケーブル防護のための専門機関の設置、民間通信事業者及び国際ケーブル保護委員会並びに各国海軍との連携、そして海底通信ケーブル防護のための国際ルール作りへの参画を提言したい。

現在、日本と世界を結ぶ海底通信ケーブルが張りめぐらされた南シナ海において、熾烈なハイブリッド戦(Hybrid Warfare)が日夜繰り広げられている。それは、2006年のレバノン戦争において武装組織ヒズボラによる通常戦、不正規戦、テロ行為など異なる戦闘方式を組み合わせた戦争様相を意味し、それによってイスラエル軍は完敗を喫したことから、最近ではロシア系住民によるクリミアのウクライナからの分離独立運動や中国の漁船に扮した海上民兵活動に受け継がれている⁶¹。それでは、わが国は、このようなハイブリッド戦に、いかに対応すべきであろうか。かつて、現役時代にストラテジック・コミュ

ニケーションを強力に推進したスタヴリディス（James Stavridis）米海軍退役大将（タフツ大学フレッチャースクール法律外交大学院学長）は、南シナ海での中国による武装漁船による不法行為と政府のソーシャルネットワーク戦術を組み合わせた海上ハイブリッド戦を想定した上で、その対応策として、①海上ハイブリッド戦の研究の促進、②戦術的・技術的対応能力の向上、③諜報・情報収集及び国際間・官民間協力の促進、④同盟国等との連携強化、⑤海上ハイブリッド戦に対する教育訓練（リムパックを含む）、⑥米沿岸警備隊の強化の6項目を提唱している⁶²。なお筆者は、レバノン戦争において、拉致された兵士の救出という限定作戦に固執した結果、事態が本格的戦争に発展していることを見抜けず、受動的対応に終始したイスラエルの教訓を踏まえ、ハイブリッド戦においては常に通常戦を予期して対応する必要性も強調したい。因みに新たな防衛大綱が、純然たる平時でも有事でもないグレーゾーン事態を想定し、政府が一体となってシームレスに対応する考えを強調していることは適切である⁶³。そして、ストラテジック・コミュニケーションの観点から、現場海域においてグレーゾーンを作り出している戦場の霧（fog of war）を払拭し、そこで起きている事件の実相を逸早く世界に知らしめて国際世論を喚起することが、わが国にとって有利な紛争終結への近道ではないかと考える。そのための有力な武器となるのが世界をつなぐインターネットであり、それを支える海底通信ケーブルの防護こそが海洋ストラテジック・コミュニケーションというわが国の新たな海の安全保障政策を実現させてくれるに違いない。

今から約120年前の日清戦争において、わが国は朝鮮半島中部西岸の豊島沖で発生した高陞号事件に直面し、当時の陸奥外相は、英国政府の意を汲み早期終結を急ぐ在英公使の建議を退け、法制局長官を佐世保鎮守府に派遣して事実調査を行い、国際法上、日本海軍の行為が正当であることを明らかにするとともに、英国の著名な国際法学者の支持も得て事件を無事に終局させ、中立国英国との関係悪化を回避したのみならず、日本に対する国際的評価を高める結果をもたらした⁶⁴。因みに、前掲のスタヴリディス退役海軍大将は、ストラテジック・コミュニケーションの指針の筆頭に「真実を語れ（Tell the Truth）」という言葉掲げ、それがすべてに通じる絶対的な基本原則であると強調している⁶⁵。これを踏まえるならば、当時の日本は海洋ストラテジック・コミュニケーションの先駆者として、そのあるべき姿を示したといえるかもしれない。

注

¹ David E. Sanger and Eric Schmitt, “Russian Ships Near Data Cables Are Too Close for U.S. Comfort,” *The New York Times*, October 25, 2015, <https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html> (2017年10月24日). なお、海底通信ケーブルへの攻撃や盗聴の歴史は古く、第1次世界大戦において英国はドイツの海底通信ケーブルを切断したほか、盗聴によりドイツの諜報活動を阻止したとされる（Robert K. Massie, *Castles of Steel : Britain,*

Germany and the Winning of the Great War at Sea, Vintage, London, 2003, p.77及び Mark M. Lowenthal, *Intelligence : From Secrets to Policy, Fourth Edition*, CQ Press, Washington,D.C. 2009, pp.90-91)。また、米ソ冷戦時代にはオホーツク海を舞台に日本の海底通信ケーブルにも関わる盗聴活動が計画されたという (Sherry Sontag and Christopher Drew with Annette Lawrence Drew, *Blind Man's Bluff : The Untold Story of Cold War Submarine Espionage*, arrow books, 1998, p.247)。

² Sanger and Schmitt, op.cit.

³ Doug Bernard, "Why Is Russia Interested in Undersea Internet Cables ?," VOA News, November 06, 2015, <https://www.voanews.com/a/russia-interest-in-undersea-internet-cables-raises-alarm/3044819.html> (2017年10月24日)。

⁴ David B. Larter, "Navy grapples with Russian threats to undersea cables," *Navy Times*, October 30, 2015, <https://www.navytimes.com/news/your-navy/2015/10/30/navy-grapples-with-russian-threats-to-undersea-cables> (2017年10月24日)。なお、スタヴリディス米海軍退役大將も、国と国際機関は国際犯罪組織やテロリストによる大規模なケーブル切断のシナリオを共同で考え、防衛する方法を研究すべきであると述べるに止まっている (James Stavridis, *Sea Power : The History and Geopolitics of the World's Oceans*, Penguin Press, 2017, p.323)。

⁵ 光海底ケーブル執筆委員会『光海底ケーブル』パレード発行、2010年、28頁。Bernard, op.cit.

⁶ Asia-Pacific Economic Cooperation, APEC Policy Support Unit, Economic Impact of Submarine Cable Disruptions, December 28, 2017, pp.9・23, <https://www.apec.org/Publications/2013/02/Economic-Impact-of-Submarine-Cable-Disruptions> (2017年12月28日)。

⁷ Douglas R. Burnett, "Cable Vision," *Proceedings*, U.S. Naval Institute, August 2011, pp.69・70~71。

なおケーブル敷設船は、敷設及び修理作業の特性から低速航行あるいは洋上で停船することが多く、他の船舶に比べ海賊や強盗の格好の標的になるといわれる (Mick Green and Douglas Burnett, "Protecting Cables in Cable Operations," D.R.Burnett, Robert G. Beckman and Tara M. Davenport eds., *Submarine Cables : The Handbook of Law and Policy*, Martinus Nijhoff Publishers, 2014, p.233)。

⁸ Commander Michael Matis, U.S. Navy, "The Protection of Undersea Cables : A Global Security Threat," USAWC Strategy Research Project, 07 March 2012, pp.17~18, www.dtic.mil/get-tr-doc/pdf?AD=ADA 561426 (2017年12月11日)。

⁹ 土屋大洋「サイバーセキュリティと国際政治」『ニューズウィーク日本版』2015年10月27日、www.newsweek-japan.jp/tsuchiya/2015/10/post-6_2.php及び同「日米サイバーセキュリティ協力の課題」笹川平和財団日米安全保障専門家会議軍事安全保障ワー

キンググループ1報告書、2016年3月、4～5頁、https://www.spf.org/topics/WG1_report_Tsuchiya.pdf（いずれも2017年11月20日）。また、武井良修・海洋政策研究財団研究員も、国際通信網の寸断・混乱を狙ったテロリストによる海底通信ケーブルへの攻撃の危険性に言及しているものの、国際的な管理法制の整備の必要性を指摘するに止まり、具体的な政策提言にまでは至っていない（同「国際海底ケーブル管理法制の整備を」海洋政策研究所Ocean Newsletter第222号、2009年11月5日、https://www.spf.org/opri-j/projects/information/newsletter/backnumber/2009/222_1.html（2017年12月9日）。なお、伊東寛・経済産業省サイバーセキュリティ・情報化審議官は、サイバー攻撃への対策の一環として「海底ケーブル陸揚げ所に関所を設けて、ここをサイバー的に守るだけでかなりの防衛が可能」と述べているが、海底通信ケーブルの防護については触れていない（同「連載サイバースペースとセキュリティー 第6回セキュアな文化形成へ：経産省サイバーセキュリティ審議官としての挑戦」『情報管理』Vol.59, No.12（2017年3月）、851頁、https://www.jstage.jst.go.jp/article/johokanri/59/12/59_849/_pdf/-char/ja（2018年1月4日））。

- ¹⁰ 土屋、前掲「日米サイバーセキュリティ協力の課題」4頁。
- ¹¹ 光海底ケーブル執筆委員会、前掲書、71～73頁。因みにOS/OFSケーブルの破断荷重は98kN（キロニュートン、以下同じ）であり、米国で開発された光海底ケーブルの破断荷重（SL17=79kN及びSL21=107kN）に比べ、大差はない。（同書、72・74頁）。新納康彦「太平洋1万キロ決死の海底ケーブル“国際光海底ケーブルネットワーク”」『武蔵工業大学環境情報学部情報メディアセンタージャーナル』2006.4 第7号、64頁、www.yc.tcu.ac.jp/~cisj/07/07_08.pdf（2017年12月4日）。
- ¹² 光海底ケーブル執筆委員会、前掲書、280～288頁。なお現在、埋設は漁業が行われる水深1,000m程度までとされ、埋設機による溝の深さは3mに達するものもあるという（太田努・西山友久「光海底ケーブルのルート設計及び敷設技術」『NEC技報』Vol.62 No.4/2009、51頁、jpn.nec.com/techrep/journal/g09/n04/pdf/090411.pdf（2017年12月4日））。
- ¹³ 光海底ケーブル執筆委員会、前掲書、343～345頁。
- ¹⁴ 同、80・243～244頁。
- ¹⁵ 同、276～279頁。なお海底通信ケーブルシステムは、通常二か国以上の通信事業者によって計画され、当事者間の合意による建設保守協定で定められた保守責任者の重要な役割に、漁業関係者、水路関係者、中央官庁、地方自治体などに対するケーブル保護活動があり、漁業関係者等との間で意思疎通や周知・広報・定期連絡が行われている（同、343～346頁）。
- ¹⁶ 海底通信ケーブルの敷設等の事業を手掛けるNTTワールドエンジニアリングマリンの高瀬充弘氏は、第1期海洋基本計画では、海底通信ケーブルについて、ほとんど触れられていないとした上で、次のように述べている。「何しろ物資の海上輸送と

は違い、情報の輸送は海底深く沈められたケーブルの中を電子信号が行き交うだけで、人の目には触れませんので、なかなかその存在を認識していただけません。ただ、この海底輸送路（海底ケーブル）が一度、故障すると、日本と外国とのコミュニケーションが遮断され、経済・社会活動に大きな影響を引き起こします」（高瀬「海洋基本計画と情報の“海底”輸送の確保」海洋政策研究所Ocean Newsletter第190号、2008年7月5日、https://www.spf.org/opri-j/projects/information/newsletter/backnumber/2008/190_2.html（2017年12月4日））と述べている。

- 17 総合海洋政策本部決定『我が国の海洋状況把握の能力強化に向けた取組』2016年7月26日、www.kantei.go.jp/jp/singi/kaiyou/dail5/shiryou1_2.pdf（2017年12月3日）。またわが国のMDAの取組については、内閣府総合海洋政策推進事務局長・甲斐正彰『我が国の海洋政策の現状と今後の課題』24～29頁を参照（公益財団法人笹川平和財団 海洋政策研究所 第141回海洋フォーラム、2017年4月25日、https://www.spf.org/opri-j/projects/141_Ocean_Forum_Presentation.pdf（2017年12月3日））。
- 18 前掲『我が国に海洋状況把握の能力強化に向けた取組』、1頁。
- 19 海洋状況把握に係る関係府省等連絡調整会議『我が国における海洋状況把握（MDA）について』2015年10月、https://www.kantei.go.jp/jp/singi/kaiyou/mda/mda_concept.pdf（2017年12月3日）。
- 20 内閣官房「海上保安体制強化に関する関係閣僚会議議事録」2016年12月21日、1～2頁、<https://www.kantei.go.jp/jp/singi/kaihotaisei/dail/gijiroku.pdf>（2017年12月16日）。なお、関係閣僚会議では『海上保安体制強化に関する方針』が決定されたが、海底通信ケーブルの防護は想定されていない。
- 21 防衛省『平成29年版防衛白書』358～361頁、www.mod.go.jp/j/publication/wp/wp2017/pdf/290301_02.pdf（2018年1月4日）。
- 22 光海底ケーブル執筆委員会、前掲書、343・346～347頁。因みに、太平洋・インド洋には横浜ゾーン（母港：横浜、釜山、上海、保守船：2隻）、北米ゾーン（母港：ポートアイランド、保守船：1隻）、SEAIOCMAゾーン（母港：マニラ、シンガポール、インド／コチン、保守船3隻）がある（同、348頁）。
- 23 同、350頁。2015年現在、日本のICPC会員は、NTTコミュニケーションズ、KDDI、SoftBankテレコム、NEC、海洋研究開発機構、東京大学地震研究所、国際ケーブル・シップ株式会社、防災科学技術研究所の8団体である（ICPC Member List, Update Monday 05 February 2018, <https://www.iscpc.org/about-the-icpc/member-list/>（2018年2月11日））。
- 24 A presentation to APEC by Mr. Mick Green (ICPC Chairman), Mr. Stephen Drew (ICPC Executive Committee Member), Professor Lionel Carter (ICPC Marine Environmental Adviser) and Mr. Douglas Burnett (ICPC International

Cable Law Adviser) , “Submarine Cable Network Security,” Submarine Cable Protection Information Sharing Workshop, Singapore 13 April 2009, www.iscpc.org/documents/?id=138 (2017年12月10日)。

²⁵ The White House, Presidential Policy Directive-Critical Infrastructure Security and Resilience, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (2017年12月24日)。ブレッシー (Kent Bressie) 海底通信ケーブル作業部会共同部会長は、その共著論文において「行政命令や大統領政策指示は特に言及していないが、この定義は明らかに海底ケーブル・システムを含む」と述べている (K.Bressie & Madeleine Findley, “Cyber-security Developments Raise Growing Regulatory Concerns For Undersea Cable Industry,” *Submarine Telecoms Forum*, Issue #69, March 2013, p.10, www.subtelforum.com/articles/wp-content/STF_69.pdf (2017年12月24日))。

²⁶ Michael Sechrist, “Cyberspace in Deep Water : Protecting Undersea Communication Cables By Creating an International Public-Private Partnership,” Harvard Kennedy School, March 23, 2010, pp. 28-29, https://www.belfercenter.org/sites/default/files/files/publication/PAE_inal_draft_-_043010.pdf (2017年12月17日)。

²⁷ Andrew D. Lipman, Ulises R. Pin & Catherine Kuersten, “Regulatory and National Security Concerns for Submarine Cable Construction,” *Submarine Telecoms Forum*, Issue #87, March 2016, pp.32-34, www.subtelforum.com/STF-87/mobile/index.html?doc=A3FD0DCD44665F5E8BDAC8764C949FA6 及び Michael Sechrist, “New Threats, Old Technology : Vulnerabilities in Undersea Communications Cable Network Management Systems,” Harvard Kennedy School Belfer Center for Science and International Affairs, February 2012, p.16, <https://www.belfercenter.org/sites/default/files/files/publication/sechrist-dp-2012-03-march-5-2012-final.pdf> (2017年12月18日)。なおチーム・テレコムについては、現在、安全保障と規制緩和の両立の観点から審査期間の短縮が議論されている (Andrew D. Lipman, Ulises R. Pin & Stephany Fan, “Streamlining the “Team Telecom” Review for Submarine Cables,” *Submarine Telecoms Forum*, Issue #93, March 2017, p.21, https://issuu.com/subtelforum/docs/stf_93 (2018年1月3日))。

²⁸ Public-Private Analytic Exchange Program 2017, U.S. Department of Homeland Security, Office of the Director of National Intelligence, *Threats to Undersea Cable Communications*, September 28, 2017, pp.7-8, <https://www.dni.gov/files/PE/Documents/1-2017-AEP-Threats-to-Undersea-Cable-Communications.pdf> (2018年7月29日)。なお、チームは、国土安全保障省、国家情報長官室、FBIの政府関係者6名とブリティッシュ・テレコムなど民間通信及びセキュリティ企業の関係者4名の計10名

で構成。

²⁹ *Ibid.*,p.15.

³⁰ 英国については、The Secretary of State for Defence, The UK National Strategy for Maritime Security, HM Government, May 2014, p.32, <https://www.gov.uk/government/publications/national-strategy-for-maritime-security> (2018年3月6日)を、沿岸防護地帯については、Australian Communications and Media Authorityの海底ケーブル防護のホームページ (<https://www.acma.gov.au/industry/Telco/infrastructure/Submarine-cabling-and-protection-zones> (2018年7月29日)) を、それぞれ参照。

³¹ Rishi Sunak, "Undersea Cables : Indispensable, insecure," *Policy Exchange*,2017,p.18, <https://policy-exchange.org.uk/publication/undersea-cables-indispensable-insecure/> (2018年3月6日)。

³² Coli E. Dauber, "The Truth is out there : Responding to Insurgent Disinformation and Deception Operations," *Military Review*, January-February 2009, pp.13-14, usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20090228_art005.pdf (2018年1月27日)。

³³ Daniel Kimmage and Kathleen Ridolfo, *An RFE/RL Special Report : Iraqi Insurgent Media-The War of Images and Ideas*, June 2007, pp.42-55, <https://docs.rferl.org/archive/online/OLPDFfiles/insurgent.pdf> (2018年1月28日)。なお同報告書によれば、2007年3月の1か月間に武装勢力が発信した声明は966件に上り、これとは別に米軍への攻撃を呼び掛ける声明は357件、またイラク政府軍に対する同様の声明は296件に達している (同、pp.8-10)。

³⁴ Cori E. Dauber, "YouTube War : Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer," Strategic Studies Institute, November 2009, pp.11-12, <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=951> (2018年1月28日)。

³⁵ DMA, *Defense Media Activity 2016 Annual Report*, Fort Meade, Maryland, Calendar Year 2016, pp.3- 6・16-17, www.dma.mil/Portals/0/Documents/DMA-2016-AnnualReport.pdf (2018年1月29日)。また米国のストラテジック・コミュニケーションについては、拙稿「米国のストラテジック・コミュニケーション政策」『国際公共政策研究』第15巻第1号 (2010年9月) を参照。

³⁶ NATO Strategic Communications Centre of Excellence, *Report for the period from 1 October 2014 to 31 December 2014*, Riga, Latvia, 31 March 2015, 同, *Audited Annual Report 2015*, 同, *Audited Annual Report 2016*, <https://www.stratcomcoe.org/annual-reports> (2018年2月25日)。なお同センターは、ラトヴィアの首都リガに設置され、エストニア、ドイツ、イタリア、ラトヴィア、リトアニア、ポーランド、英国がスポンサー国となっている。

- ³⁷ Ibid., p.14及びDIMOC-JCCCホームページを参照。またCOMCAMに関する邦語文献として、前山一歩「海上自衛隊広報の課題と挑戦－米軍広報との比較から」『海幹校戦略研究』第3巻第1号（2013年5月）を参照。
- ³⁸ Department of Defense, Department of Defense Instruction 5040.02 : Visual Information (VI) , October 27,2011,Incorporating Change 1,Effective July 8,2016, <https://www.hsdl.org/?abstract&did=794356>及びDepartment of Navy, Office of the Chief of Naval Operations, OPNAVINST 3104.1A : Navy Visual Information Program Policy and Responsibilities, 9 Oct 09, pp.1-1・2-2,navybmr.com/study%20material/OPNAVINST%203104.1.pdf（いずれも2018年2月2日）。
- ³⁹ Department of the Navy, Office of the Chief of Naval Operations, OPNAVINST 3104.3A : Navy Combat Camera Program Policy, Responsibilities, and Procedures, 31 Aug 2010, p.2, https://fas.org/irp/doddir/navy/opnavinst/3104_3a.pdf（2018年2月1日）。
- ⁴⁰ Ibid.
- ⁴¹ Department of the Navy, Office of the Secretary, SECNAVINST 5720.44C CH-1 : Department of the Navy Public Affairs Policy and Regulations, October 14, 2014, 1-4, www.jag.navy.mil/distrib/instructions/SECNAVINST5720.44CPublicAffairsPolicyRegulations.pdf（2018年2月3日）。
- ⁴² Christopher Paul, *Strategic Communication : Origins, Concepts, and Current Debates*, Praeger, 2011, pp.45及びJoint Chiefs of Staff, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 (As Amend Through 12 July 2007) , pp.54・178・342・462, <https://wikileaks.org/w/Images/a/a7/Jp1-02.pdf>（2018年3月5日）。なお、2010年版の『軍事用語辞典』では、プロパガンダに関する用語は一切掲載されていない。
- ⁴³ Edward Hallett Carr, *The Twenty Years' Crisis 1919-1939 : An Introduction to the Study of Inter- national Relations*, Harper Perennial, 1964, pp.132-145、近衛文磨『戦後欧米見聞録』中公文庫、昭和56年、41～42頁。
- ⁴⁴ 宮尾恵美「尖閣諸島海域漁船衝突事件についての中国外交部発言（3）」『外国の立法』国立国会図書館調査及び立法考査局、2011年1月、www.ndl.go.jp/jp/diet/publication/legis/pdf/02460112.pdf（2017年11月28日）。また、ビデオ映像を投稿した海上保安官は、その著書で「正直、反応の大きさは予想していたが、情報伝達の速さは予想を遥かに超えたものであった。」と述べている（一色正春『何かのために sengoku38の告白』朝日新聞出版、2011年、10頁）。
- ⁴⁵ 防衛省『平成29年版防衛白書』343頁。なお、国際法上、外国潜水艦が沿岸国の接続水域内を潜没航行することは禁じられていないが、海上自衛隊は2018年1月11日午前、尖閣諸島（大正島）の接続水域内を潜没航行する潜水艦と海上を航行する中国

海軍艦艇を確認・追尾し、その翌日当該潜水艦が東シナ海海上を中国国旗を掲げて航行する映像写真を防衛省のホームページで公表している（www.mod.go.jp/j/press/news/2018/01/index.html（2018年2月6日））。

- ⁴⁶ Catherine Creese, “The U.S.Naval Seafloor Cable Protection Office “Call Before You Dig!”” *Submarine Telecoms Forum*, Issue No 29, p.35, www.subtelforum.com/issues/Issue%2029.pdf（2018年2月6日）。因みに、NSCPOのホームページによれば、米海軍は4万カイリ以上に及ぶケーブルを保有している（https://www.navfac.navy.mil/products_and_services/ci/products_and_services/naval_ocean_facilities_Program/sea_floor_cable_protection_nscpo.html）。

- ⁴⁷ Creese, *op.cit.*, pp.35-36.

- ⁴⁸ Bob Fredrickson & Catherine Creese, “Navy Undersea Cable Systems,” *Submarine Telecoms Forum*, Issue No 35, November 2007, pp.39-41, www.subtelforum.com/issues/Issue%2035.pdf（2018年2月6日）。

- ⁴⁹ 大井篤『海上護衛戦』朝日ソノラマ、1983年、44頁。

- ⁵⁰ 支援機構は、2017年1月にNECとともに、香港～グアム間の光海底ケーブル事業に参画し、最大約58億円を出融資し、また同年11月にも同じくNECとともに日本～グアム～豪州間の光海底ケーブル事業に参画し、最大4,450万米ドルを出融資することが総務省によって認可された（総務省報道資料、平成29年1月20日付及び同年11月28日付、www.soumu.go.jp/menu_news/s-news/01tsusin01_02000213.html及びwww.soumu.go.jp/menu_news/s-news/01tsusin06_02000106.html（いずれも2018年2月10日））。

- ⁵¹ 総務省告示第412号、平成27年11月30日、www.soumu.go.jp/main_content/000388382.pdf（2018年2月10日）。

- ⁵² 株式会社海外通信・放送・郵便事業支援機構ホームページの会社概要を参照、www.jictfund.co.jp/about/Company（2018年2月10日）。

- ⁵³ 総務省国際戦略局『世界に貢献する総務省アクションプラン～総務省海外展開戦略～概要』2018年2月、5頁。

- ⁵⁴ ICPC, Member List, Updated Monday, 6 August 2018, <https://www.iscpc.org/about-the-icpc/member-list/>（2018年8月11日）。Greese, *op.cit.*, pp.35-36.

- ⁵⁵ Public-Private Analytic Exchange Program 2017, *op.cit.*, pp.11-12. なお、総務省の『海外展開戦略（情報通信）』（平成29年10月）によれば、海底ケーブルの世界シェア（2014年）は、米国企業34%、日本企業30%、欧州企業21%、その他15%となっている。

- ⁵⁶ Michael N. Schmitt, General Editor, *Tallinn Manual on the International Law applicable to Cyber Warfare : Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge University Press, 2013, p.250.

- ⁵⁷ *Ibid.*

- ⁵⁸ Michael N. Schmitt, General Editor, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations : Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge University Press, 2017, p.252.
- ⁵⁹ *Ibid.*, xiii. なお『タリン・マニュアル2.0』の国際法専門家グループには、日本から東京大学の中谷和弘教授が参加している。
- ⁶⁰ *Ibid.*, xii-xxii.
- ⁶¹ ハイブリッド戦については、Frank G. Hoffman, “Conflict in the 21st Century : The Rise of Hybrid Wars,” *Potomac Institute for Policy Studies*, December 2007及び拙稿「対反乱作戦研究の問題点と今後の動向について」『防衛研究所紀要』第14巻第1号（2011年12月）を参照。
- ⁶² Admiral James Stavridis, U.S.Navy (Retired) , “Maritime Hybrid Warfare Is Coming,” *Proceedings Magazine* Vol.142/12/1, 366, December 2016, <https://www.usni.org/magazines/proceedings/2016-12-0/Maritime-hybrid-warfare-coming>（2017年10月24日）。
- ⁶³ 『平成31年度以降に係る防衛計画の大綱』国家安全保障会議・閣議決定、平成30年12月18日、2～3・8頁、<https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218.pdf>（2019年1月22日）。
- ⁶⁴ 陸奥宗光『蹇蹇録』岩波文庫、1983年、140～148頁。
- ⁶⁵ James Stavridis, “Strategic Communication and National Security,” *Joint Force Quarterly*, Issue 46, 3rd quarter 2007, p.5, www.dtic.mil/get-tr-doc/pdf?AD=ADA575204（2018年2月18日）。