海底ケーブルをめぐる地政学的・地経学的状況

慶應義塾大学
土屋 大洋*

日本は海に囲まれており、国際通信の 99%は海底ケーブルを経由するといわれている。残りの 1%は人工衛星だが、海底ケーブルで安価な大容量通信が可能になっているのに対し、人工衛星の利用は高価で、通信容量も少ない。サイバー攻撃の多くが海外から来ていることを考えると、海底ケーブルを通じてほとんどの悪意ある通信が行われているといって良い。しかし、その通信量はあまりに多く、その通信を監視するのは極めて困難でもある。

本稿では、能動的サイバー防御において期待される通信情報の利用のうち海底ケーブルの監視が将来的に行われる可能性があることを視野に入れながらも、その直接的な応用の前提となる地政学的・地経学的状況について検討したい。

1．海底ケーブルの経済安全保障

海底ケーブルの一連のシステムは、水中部分にあたるウェット・プラントと、陸上部分にあたるドライ・プラントに大別される。ウェット・プラントは、ケーブルそのものと、およそ 50 キロメートル毎に設置される中継器から成る。

海底ケーブルのシェアについては諸説あるが、海底ケーブル業界をウォッチしているテレジオグラフィー社と経済産業省によれば、フランスのアルカテル・サブマリン・ネットワークス（ASN）社が 40%、米国のサブコム社が 31%、OCC 社を保有する日本の NEC が 21%とされる。大手 3 社を追いかける形で中国の HMN テックが 8%のシェアを持っている[1]。

4 社は世界各地で進む海底ケーブル・プロジェクトにおいて競争を繰り広げている。しかし、HMN テックが中国政府から補助金を受け、不公正な競争を行っているとする業界関係者は少なくない。また、HMN テックのケーブルには地経学的なリスクがあるとの声も根強い。同社のルーツの一つが中国のファーウェイ（華為技術）社だからである。

しかし、海底ケーブルそのものは光ファイバーを保護するとともに電気を通す金属部分で覆った構造であり、セキュリティ・リスクを仕込むのは難しい。海底でデータを第三者が取得することも極めて困難であり、実証されてはいない。

海底ケーブルは、ある程度水深のあるところでは海底にそのまま横たわっている。しかし、漁網や錨等によって損傷の可能性がある沿岸部では海底の砂の中に埋められていることが多い。地下から陸揚局に引き込まれたケーブルは、そこで各種の機械に接続される。PFE（Power Feeding Equipment）と呼ばれる給電装置や SLTE（Submarine Line Terminal Equipment）と呼ばれる端局装置等である。

海底ケーブルの製造業者が世界で 4 社なのに対し、SLTE の製造業者は数多い。日本の NEC、三菱電機、米国のシエナ（Ciena）、エクステラ（Xtera）、インフィネラ（Infinera）、欧州の

* 慶應義塾大学大学院政策・メディア研究科教授

[1]「海底ケーブルの切れにくさ実証、総務省が支援 GAFA から受注狙う」『日本経済新聞』2025 年 7 月 9 日電子版。

ASN、ネクサンス（Nexans）、中国の HMN テック等である。

SLTE は海底ケーブルが伝送してきた信号を処理する装置であり、仮に海底ケーブルの通信傍受が行われるとすれば、SLTE を起点とした陸揚局内部のシステムかさらに陸地の中に入った通信事業者の局舎の中ということになるだろう。

米国の第一次ドナルド・トランプ（Donald Trump）政権において、マイク・ポンペオ（Mike Pompeo）国務長官は 2020 年 8 月にクリーン・ネットワーク政策を打ち出した。ポンペオ長官は、海底ケーブルを含む通信システムが中国共産党の検閲ツールであり、米国市民の個人情報への重大な脅威だと指摘し、米国内および米国につながる通信ネットワークから中国製品を排除すると発表した。

その前年の 2019 年には米国ロサンゼルスと香港を接続予定だった PLCN（Pacific Light Cable Network）の陸揚げをトランプ政権は拒否した。PLCN は中国の鵬博士集団が出資していたが、トランプ政権の拒否後、同社は撤退し、香港ではなく台湾とフィリピンに分岐して陸揚げされることになった。

こうした米国政府の懸念は、海底ケーブルが米国のサイバーセキュリティ政策において重要な役割を果たしていることの裏返しと見ることができるかもしれない。すでに米中間でつながっている海底ケーブルは存在し、その両端でおそらく米国政府と中国政府は通信を監視している。それでも敢えて新しいネットワークを拒否したのはリスクを極小化しようという努力であるとともに、一種の政治的な示威行動ともいえるだろう。

2．海底ケーブルと能動的サイバー防御

実際に海底ケーブルは能動的サイバー防御に使われるのだろうか。

光ファイバーを中心に入れた光海底ケーブルが使われるようになったのは 1980 年代半ば以降である。1970 年代には銅線を中心に入れた海底ケーブルが使われていた。当時の海底ケーブルは、信号が通ると微弱な電波を発していたという。オホーツク海の海底に敷設されたソビエト連邦の海底ケーブルを傍受する試みが米国によって行われたことがある。

アイビーベル作戦と名付けられた試みでは、オホーツク海の海底ケーブルの脇に傍受装置を設置し、信号を記録させた。装置を定期的に回収し、記録された信号を解析することで事後的ながらソ連の通信内容を把握することができたという[2]。

しかし、現代の光海底ケーブルではケーブルの中を流れる信号は電気信号ではなく光信号であり、微弱な電波は出ないため、アイビーベル作戦のような海底での傍受は不可能だとされる。そのため、前述のようなドライ・プラントにおける傍受が行われていると見られる。

そうした措置を一気に推し進めることになったきっかけが 2001 年 9 月 11 日の対米同時多発テロであった。テロを未然に防止できなかったことから、米国家安全保障局（National Security Agency：NSA）は大規模な通信傍受を開始した。外国情報監視法（Foreign Intelligence Surveillance Act：FISA）において求められる令状を得ないで行われた「令状なし傍受」は違法の可能性があったが、ジョージ・W・ブッシュ（George W. Bush）大統領が発した秘密の大統領令に基づいて行われた。

9.11 テロを起点として拡大・発展した NSA の通信監視は海底ケーブルにも及んだ。2005 年にこれらの活動はニューヨークタイムズ紙によって報道され[3]、2013 年には民間のコントラクターとして NSA の業務を請け負っていたエドワード・スノーデン（Edward Snowden）によって暴露された[4]。

英国で NSA と同様の傍受活動を展開する政府通信本部（Government Communications

[2] シェリー・ソンタグ、クリストファー・ドルー、アネット・ローレンス・ドルー（平賀秀明訳）『潜水艦諜報戦（上・下）』新潮社、2000 年。
[3] ジェームズ・ライゼン（伏見威蕃訳）『戦争大統領―CIA とブッシュ政権の秘密―』毎日新聞社、2006 年。
[4] グレン・グリーンウォルド（田口俊樹、濱野大道、武藤陽生訳）『暴露―スノーデンが私に託したファイル―』新潮社、2014 年。

Headquarters：GCHQ）の研究で知られるリチャード・オルドリッジ（Richard Aldrich）は、9.11 発生時の NSA 長官マイケル・ヘイデン（Michael Hayden）の見解は、「私たちの周りにあるデバイスが収集するデータの量は 10 年で膨大なものになり、情報機関はコンテンツに頼らなくなり、代わりにメタデータと地理情報をもっと使うようになるだろうというものだった」と指摘している[5]。電話や電子メール、ソーシャルメディアの通信の中身よりも、誰がいつ誰と通信を行っているかを見るメタデータの解析が一挙に進み始めた。

また、メタデータの解析にはピンポイントではなく、できるだけ多くのデータへのアクセスが必要とされた。ヘイデンの後任の NSA 長官であり、初代の米国サイバー軍（U.S. Cyber Command：USCYBERCOM）の司令官にもなったキース・アレグザンダー（Keith Alexander）は、「藁の山の中から針を探すなら、藁の山全体が必要だ」と述べたという[6]。

こうした文脈の中で海底ケーブルを流れる大量のデータの傍受も、米国が行う能動的サイバー防御において重要な一部となった。スノーデンが暴露した NSA の資料では、ソーシャルメディアのデータ取得とともに、海底ケーブルの傍受も同時に行うべきだと書かれていた。

しかし、海底ケーブルの通信帯域は極めて大きい。例えば、2016 年に運用を開始した太平洋を横断する FASTER ケーブルにおいては初期設計容量として毎秒 60 テラビットが設定された[7]。24 時間では 518 万 4000 テラビットに及ぶ。こうした大量の通信を毎日取得し、分析するには高度な情報技術能力が必要であり、とても人手では間に合わない。機械による自動処理が必要である。

3．戦略的資産としての海底ケーブル

海底ケーブルは、我々の日常の情報活動を支える極めて重要なインフラである。島国である日本はそれに依存しており、それをどう防護していくかは喫緊の課題になりつつある。

能動的サイバー防御という文脈では、海底ケーブルを通じて日本に流入する不正な通信をいかに見つけるか、さらには、日本国内で感染したコンピュータ・ウイルス等から発信される通信等も捕捉できるかが課題である。

日本は地理的に見てユーラシア大陸の東側に位置し、米国西海岸からアジアへつながる海底ケーブルの中継点でもある。さらに言えば、東アジア、米国、欧州、中東、インド、東南アジアを通って世界を一周する大きな光通信の帯に位置する。そうした地域には人口が多く、活発な経済に伴うサイバーセキュリティ上の懸念も多い。そうした地政学的・地経学的な状況に鑑み、日本の能動的サイバー防御能力の向上においては同盟国米国だけでなく、友好国との国際連携もまた重要な課題である。

本稿は、東京海上ディーアール株式会社が運営する調査研究プロジェクト「サイバー安全保障と能動的サイバー防御（ACD）」の成果の一部です。
https://www.tokio-dr.jp/thinktank/acd/

[5] Richard Aldrich, *GCHQ*, New York: Harper Press, 2010 (Kindle Edition), p. 545.
[6] Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, Simon & Schuster, 2016 (Kindle Edition), p. 195.
[7] 日本電気株式会社「NEC、日米を結ぶ太平洋横断大型光海底ケーブル「FASTER」の建設を完了」日本電気株式会社 <https://jpn.nec.com/press/201606/20160629_02.html>、2016 年 6 月 29 日（2025 年 7 月 19 日アクセス）。