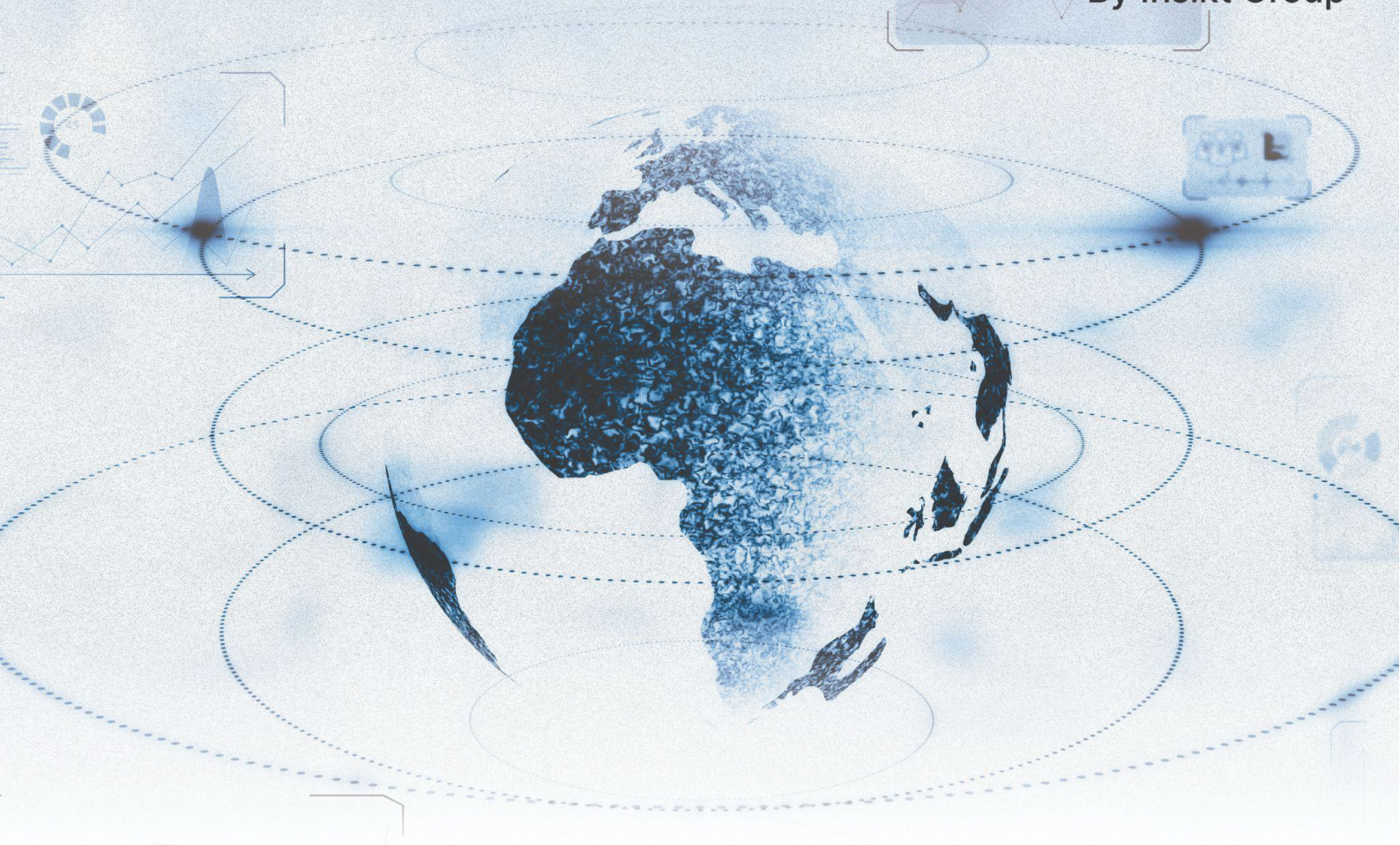
Recorded Future®

By Insikt Group®



海底ケーブルを取り巻く世界中でのリスクの高まり

TA-2023-XXXX

要約

超高速通信網を構築し、世界中での通信に使われている海底ケーブルは、世界経済の基盤です。そのリスク環境はますます複雑かつ動的なものになっています。モバイルユーザーとクラウドコンピューティングによるデータの使用量の増加と、Amazon、Google、Meta、Microsoft などのハイパースケーラーのビジネスの事情により、海底ケーブルネットワークは迅速に拡大および進化しています。地政学的な脅威、物理的な脅威、サイバー脅威が収斂するなか、海底ケーブルネットワークはそれらの脅威に対処する必要があります。

意図的な破壊とスパイ活動に関しては、高い能力と戦略的な動機を持つ国家アクターが最大の脅威であることは確実です。ハクティビストやランサムウェアグループなど、国家以外のアクターは比較的能力が乏しく、海底ケーブルのネットワークや運用システムに脅威をもたらす可能性も低いと考えられますが、そのリスクは軽視できません。船の錨や漁船によって偶発的な損害が生じることはよくありますが、その影響は大きなものではありません。

地政学的な動向として重要なものは、近い将来のリスク環境に大きな影響を与える可能性が高いと言えます。たとえば、ロシアとウクライナの戦争、中国による台湾への威圧的な行動と、可能性が指摘されている台湾の強制的な統一に向けた準備、中国政府と米国政府の関係悪化などがこれに該当します。ケーブルの所有者およびサービス事業者として中国の国有企業が果たす役割が大きくなったことで、インターネットのアーキテクチャが再構築されるなかでのデジタル監視の懸念が高まっています。ウクライナを支援する西側諸国に損害を与えたいと考えているロシアは、海底ケーブルシステムの地図を作成する意思の高まりを明らかにしています。これは海底ケーブルシステムの破壊や混乱が目的と考えられます。また、帯域幅の拡大が絶えず求められることから、ケーブルシステムの事業者は高度なネットワーク管理システムを導入しています。これはサードパーティの脆弱性を悪用するサイバー攻撃につながる可能性があります。

主な調査結果

- 世界中の金融、通信、政府の意思決定と軍事作戦がインターネットベースの接続に依存する傾向が強まっているため、海底ケーブルはインテリジェンスの収集または破壊の魅力的な標的となっています。
- 海底ケーブルの敷設、所有、運用における中国企業の役割が拡大したことで、ケーブルを利用する国家や企業にとっては、スパイ活動を行われるリスクが高まっています。
- Amazon、Google、Meta、Microsoft などのハイパースケーラーは、キャパシティを購入する立場から、海底ケーブルを直接所有する立場へと変化しました。これによって、ケーブルを敷設する新しいインセンティブがもたらされるとともに、市場の独占やデジタル主権に関する新しい懸念も生じています。歴史的に十分なサービスが提供されてこなかった地域では特に懸念が持たれています。
- ロシアとウクライナの戦争は継続中で、中国は可能性が指摘されている台湾の強制的な統一に向けた準備を進めています。また、米国と中国の二国間の関係は悪化しています。こうした事情から、米国と西側の同盟国による、経済、外交、国家安全保障の目標達成を妨げる目的で、海底ケーブルシステムに対する物理的な攻撃やインテリジェンス収集の試みが増える可能性が高いと考えられます。
- 海底ケーブルの所有者と運営事業者は、効率を最大化し、コストを削減するために、サードパーティが提供するリモートネットワーク管理システムの導入を進める可能性が高いと考えられます。これにより、脅威アクターにとっては、サイバーセキュリティの脆弱性を悪用して海底ケーブルのインフラストラクチャとデータを標的とする機会が生じます。

背景

海底ケーブルは国際的な通信のために 170 年以上使われてきました。初めて使われたのは 1850 年のことで、イギリス海峡を横断するケーブルが敷設され、イングランドとフランスの間で電報が送られました。現在では、大陸間のインターネットトラフィックとデータおよび音声通信の 99%が、海底に敷設された光ファイバー海底ケーブルを通じて伝送されていると推定されています。海底ケーブルは世界経済の基幹であり、1 日あたり 10 兆ドル以上の金融取引を可能にしています。また、政府による機密情報の通信や、海外での軍事作戦の支援にも使われています。国家の安全保障に関わる重要なインフラストラクチャであり、今日の社会が正常に機能するためには欠かせません。

海底ケーブルは、衛星通信よりも高速で、安価に利用でき信頼性も高いため、インターネットの利用者とデバイスの数の急激な増加が続き、世界のネットワークで送信されるデータの量も急増するなかで、その重要性はますます高まっています。業界でのある推計によると、全世界のモバイルでのデータ転送量は、2022 年から 2030 年にかけて年平均成長率 28%ほどのペースで増加し、1 か月あたり 6 億 350 万テラバイトに達すると見られています。このようなデータトラフィックの急増に対処するために、ケーブルシステムの所有者とサービスの提供者はキャパシティを急速に拡大しています。現在では、世界で 529 のケーブルシステムが運用されていると推計されています。これは 2013 年の 2 倍以上の数です。そして、**図 1** に示すとおり、増加のペースは速まっています。

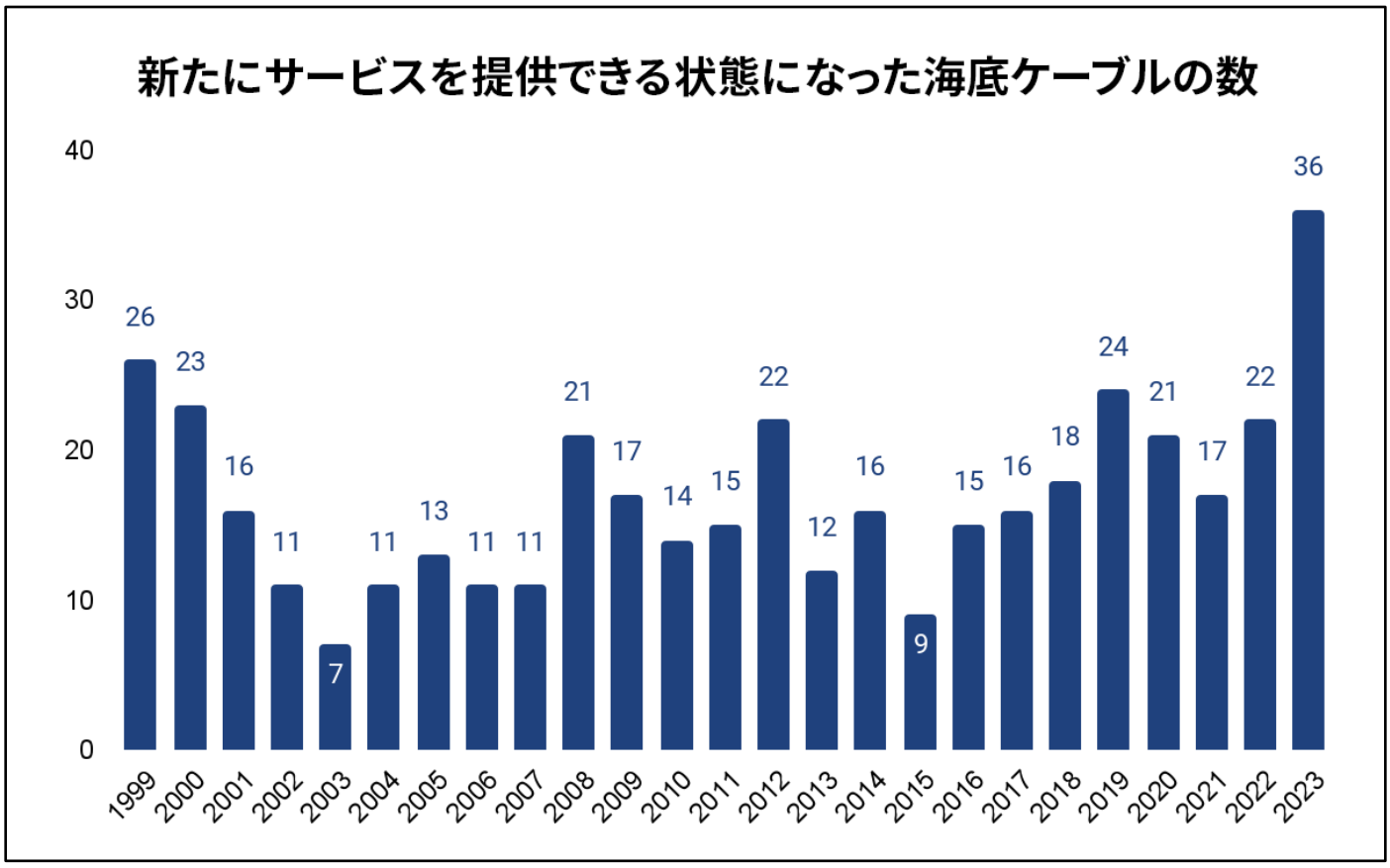
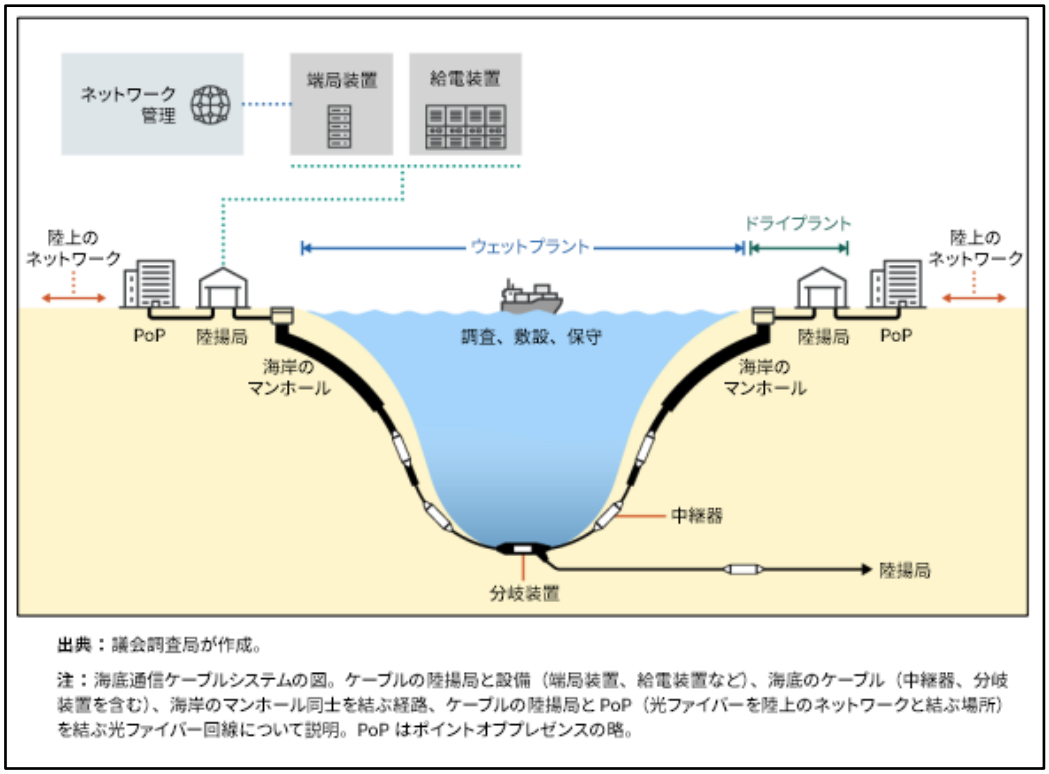


図 1：1999 年から 2023 年にかけて、新たにサービスを提供できる状態になった海底ケーブルシステムの数
（出典：Recorded Future。TeleGeography のデータを視覚化）

海底ケーブルについての基本的な説明

海底ケーブルはガラス製の精巧な光ファイバー束でできています。光ファイバーはデータを光パルスとして伝送します。プラスチック、鋼線、銅の被覆、ポリエチレンの絶縁体から成る各層で光ファイバーを包みます。水まき用ホースほどの直径のケーブルを海底の深い部分に敷設します。船の錨によって誤って傷つけられることを防ぐため、海岸線の近くではケーブルを分厚い外装に格納します。現在では、海底ケーブルに最大 24 組の光ファイバーを収められるようになっています。その帯域幅は複数の関係者が所有したり使用したりすることもあります。ケーブルの帯域幅も急激に増加しています。2003 年から利用されている、大西洋を横断する Apollo ケーブルの場合、当初の転送速度は光ファイバー1 組あたり 1 テラビット毎秒（Tbps）未満でしたが、その後の設計の変更を通じて、2015 年にはその数字が 8 テラビット毎秒まで向上しました。新しく設計されたケーブルはスループットに優れています。2023 年に敷設された、大西洋を横断する Google の Dunant ケーブルは、設計上の上限が光ファイバー1 組あたり 25 テラビット毎秒です。ただし、通常は設計上の上限の 20% ほどしか使用しません（使用されている部分を「ライトファイバー」と呼びます）。これは、需要の急増やトラフィックの再ルーティングに備えてバッファを確保するためです。

海底ケーブルシステムはウェットプラントとドライプラントの 2 つの部分に分割できます。ウェットプラントは、ケーブル自体と、信号を増幅するためにケーブルに沿って設置される中継器から成ります。ドライプラントはケーブルが沿岸に着く部分です。海岸に作られたマンホールを通じて陸揚局に到達し、地上のネットワークに接続します（**図 2**）。ケーブルの長さと構造の複雑さに応じて、陸揚局にネットワーク管理ツールと給電装置があります。たとえば、長さが 1 万 3,000 キロメートルにおよぶ Tata の TGN-Atlantic には、9,000 ボルトほどの電圧がかかっています。



出典：議会調査局が作成。

注：海底通信ケーブルシステムの図。ケーブルの陸揚局と設備（端局装置、給電装置など）、海底のケーブル（中継器、分岐装置を含む）、海岸のマンホール同士を結ぶ経路、ケーブルの陸揚局と PoP（光ファイバーを陸上のネットワークと結ぶ場所）を結ぶ光ファイバー回線について説明。PoP はポイントオブプレゼンスの略。

図 2：海底ケーブルシステム（出典：議会調査局）

世界中でのリスクの高まり

21 世紀に世界中の海底ケーブルネットワークが急速に拡大し、進化を遂げたことにより、地政学的な脅威、物理的な脅威、サイバー脅威の収斂を反映した、新しいリスクが注目されるようになりました。中国の国有企業の関与が増えたことと、ハイパースケーラー[1]の果たす役割が大きくなったことにより、ケーブルの所有の状況が変化しました。その結果、地政学の面で考慮が必要な事情が新たに生じ、インターネットの物理的なトポロジーが変化しました。ケーブルとそれに付随する陸揚局が急増し、脅威アクターがセキュリティを侵害する物理的な攻撃やスパイ活動を行う新しい機会が生じました。また、システムのキャパシティを強化するためにリモートネットワーク管理システムが導入されると、ケーブルシステムのインフラストラクチャに対するサイバー攻撃や、ケーブルで送られるデータの悪用が行われやすくなる可能性があります。

[1] ハイパースケーラーは、一般的には、特にクラウドプラットフォームとデータセンターについて、需要に応じて迅速かつ効率的にインフラストラクチャの規模を変化させる能力を持つものとして定義されます。

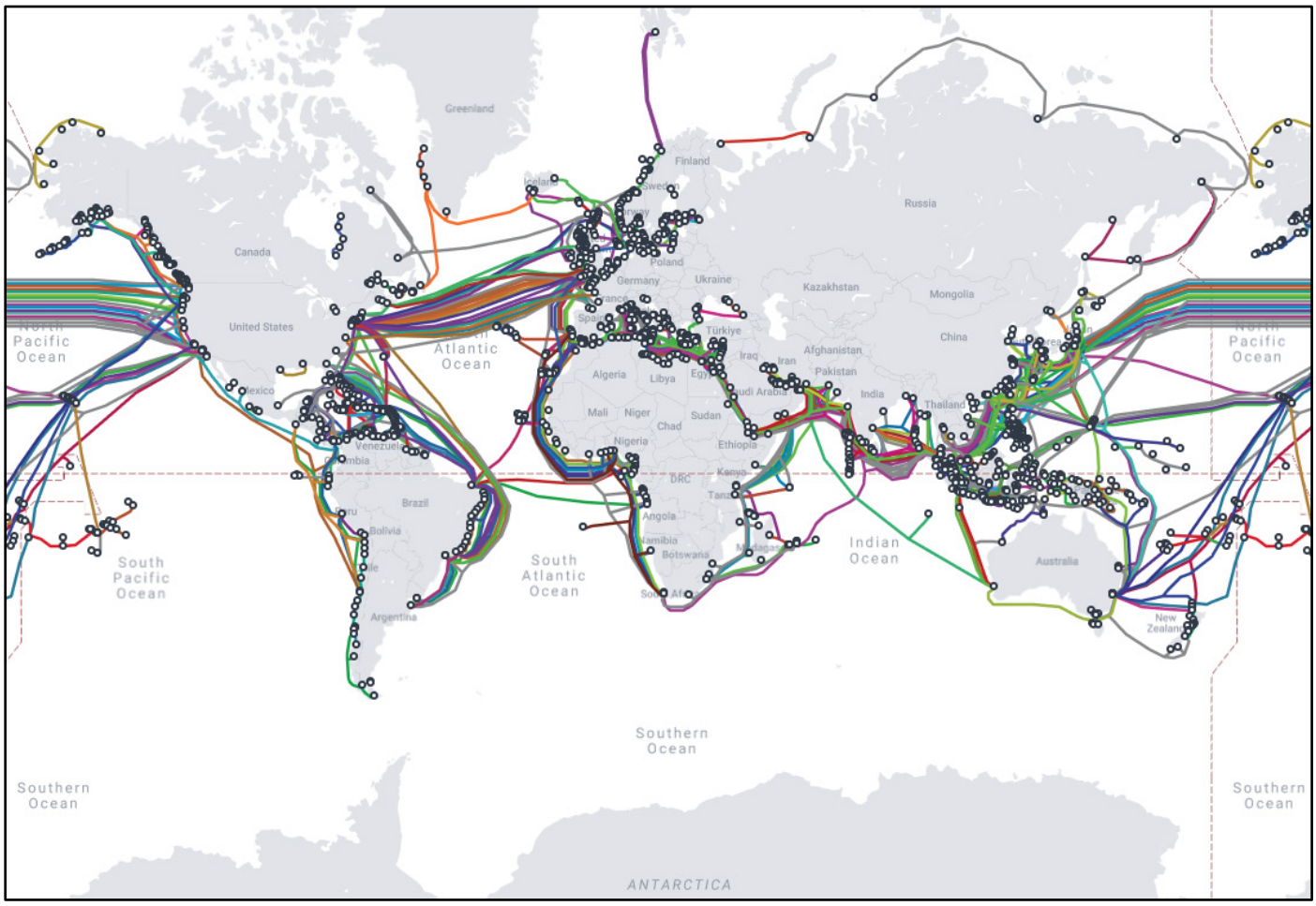


図 3：2023 年 5 月 16 日時点の海底ケーブルの地図（出典：TeleGeography による海底ケーブルの地図）

生産と所有の状況の変化

中国が関与する割合の拡大

過去 10 年間で、中国の国有企業または国家に関連する企業が、世界の海底ケーブルネットワークでの存在感を増してきました。これによって、中国が世界のデータの流れに対して操作、監視、干渉を行う能力が高まっています。海底ケーブルシステムを生産するエンティティと所有するエンティティは、通常は 2 つのグループに分かれています。従来、世界中でケーブルの製造と敷設を行ってきた大手 3 社は、米国の Subcom、フランスの Alcatel Submarine Networks、日本の NEC Corporation でした。所有についてはより分散しています。世界中の市場に広く展開すること、コストを抑えること、運用とメンテナンスの責任を分担することを目的に、1 本のケーブルを共同で所有する場合もあります。生産と所有の両面で、中国は迅速な発展を遂げています。Hengtong Optic-Electric（HMN Technologies、旧称 Huawei Marine Systems の所有者）は、ケーブルの敷設の市場で 10%のシェアを持っています。また、中国の国有通信会社である、China Mobile、China Telecom、China Unicom の 3 社は、合計で約 40 のケーブルの一部または全体を所有しています。

歴史的には、中国は中国本土、香港、台湾周辺を重視してケーブルを敷設してきました。しかし近年、中国企業は、世界中、特に東南アジア、中東、アフリカでのケーブルの敷設への関与を深めています。これは、中国の一帯一路構想（BRI）の技術的な面、しばしばデジタルシルクロードと呼ばれるものの一部として行われています。その拡大を主導しているのが Huawei Marine Systems です。この企業は、元々は中国の通信大手 Huawei と英国の Global Marine Systems のジョイントベンチャーとして誕生しました。敷設の価格が非常に安価であることから、同社については中国政府から補助金を受け取っているのではないかという憶測がなされていますが、同社はその疑いを繰り返し否定しています[2]。

Huawei は中国政府に忠誠を尽くす立場にあるため、懸念が生じています。Huawei Marine Systems は、2019 年に上海に拠点を置く Hengtong Optic-Electric に売却され、2020 年には HMN Technologies へと名称を変更しましたが、懸念は払拭されていません。Hengtong は以前に一帯一路構想のプロジェクトで中国政府と協力していたため、中国政府にとって信頼できるパートナーであると考えられます[3]。また、同社の創業者兼会長である Cui Genliang 氏は、以前は中国人民解放軍に所属する通信の専門家であったと言われています。こうしたつながりが明らかになったことを受けて、米国や西側諸国は、Huawei Marine Systems/HMN Technologies が関与するプロジェクトを取りやめたり阻止しようとしたりしています。2018 年に、オーストラリア政府は、オーストラリアと太平洋諸国を結ぶケーブルのプロジェクトから Huawei を追放しました。これは、オーストラリア保安情報機構（ASIO）がスパイ活動について懸念を示したためでした。2020 年には、ミクロネシア連邦、キリバス、ナウルを結ぶケーブルのプロジェクトに Huawei Marine Systems が参加していることについて米国が太平洋諸国に警告し、結果的にはオーストラリアの事業者がそのプロジェクトの契約を獲得しました。2021 年 12 月には、米国商務省が、制裁を目的とするエンティティリストに HMN Technologies を加えました。

それでも、世界中で海底ケーブルネットワークが拡大し続けるなかで、HMN Technologies はビジネスの機会を継続的に得ることができています。2020 年に連邦通信委員会（FCC）が公開したレポートによると、HMN Technologies（当時は Huawei Marine Systems として営業）は、それまでに世界のケーブルの約 25%を建設または修理していました。今後 2 年間で、HMN Technologies はアジアで進行中の 3 つのプロジェクトにケーブルを供給する予定となっています（**図 4**）。また、先日、中国が主導する予算 5 億ドルのケーブルネットワークが発表されました。香港、海南島、シンガポール、パキスタン、サウジアラビア、エジプト、フランスを結ぶそのネットワークにも、HMN Technologies がケーブルを供給する予定です。拡大中のこのプロジェクトは、米国が主導する SEA-ME-WE 6 ケーブルネットワークと直接競合する見込みです。HMN Technologies は、米国の強い要請により SEA-ME-WE 6 のプロジェクトから除外されました。

[2] https://www[.]huawei[.]com/en/facts/voices-of-huawei/no-huawei-isnt-built-on-chinese-state-funding
[3] https://eng[.]yidaiyilu[.]gov[.]cn/

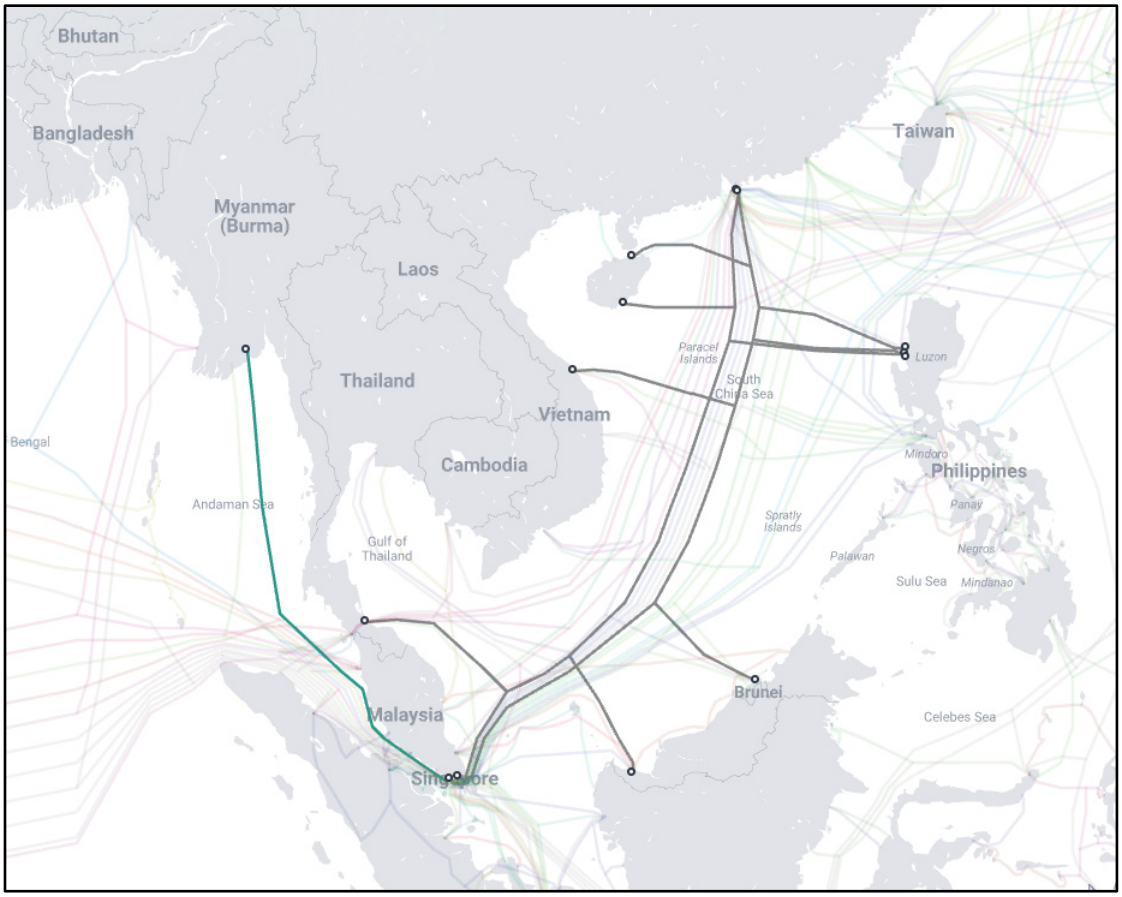


図 4：現時点で 2023 年から 2025 年にかけて予定されている HMN Technologies によるケーブルの敷設
（出典：TeleGeography による海底ケーブルの地図）

ケーブルの生産と敷設のセクターに力を入れると同時に、中国は世界中でケーブルの所有者、運営者としての役割を拡大しようとしています。この変化が進めば、中国は海底ケーブルをどこにどう敷設するかを決める能力を高めることができます。これは地政学的な目標に適うだけでなく、自身が管理する陸揚局を通じてインテリジェンスを収集する新しい機会にもつながります。また、中国政府がインターネットの物理的構造を左右する能力が向上し、その影響はデジタル面での挙動にもおよぶ可能性があります。あるアナリストの集計によると、2021 年までに、中国の国有通信会社は 3 つの海底ケーブルを所有していました（China Telecom が 2 つ、China Mobile が 1 つ）。2021 年から 2022 年のうちにその数は 34 に増加し、China Telecom、China Mobile、China Unicom が分担して所有するようになっています。

デジタルの流れを制御する中国の能力に関するこうした二重の懸念を反映して、米国は規制を積極的に課し、自国に接続するケーブルに関係する所有者グループに中国が参加することを禁じてきました。2020 年 6 月、「Team Telecom」と非公式に呼ばれる米国の省庁横断組織が、Meta と Google の申請を拒否するように FCC に提言しました。その申請では、Pacific Light Cable Network（PLCN）を通じて、ロサンゼルスとカリフォルニアから香港へと接続することになっていました。この申請に対してはさまざまな懸念が示され、たとえば米国司法省（DOJ）は、中国による「米国市民の個人的なデータを収集しようとする継続的な取り組み」と、香港をデジタルトラフィックの主要なハブにしようとしている中国の目標達成に PLCN が寄与する可能性を挙げました。

最終的に、PLCN は中国企業が所有権や陸揚局を持たない形で進められることになりました。米国本土への直接の接続を確立しようとする中国の試みはこれからも妨害されることになりそうですが、アジア太平洋地域や、アフリカをはじめとするこれまで十分なサービスが提供されてこなかった市場では、中国がネットワークの構築に成功する可能性が高いと考えられます。

- Hengtong Group の子会社が、HMN Technologies の支援を受けて、海底ケーブル Pakistan & East Africa Connecting Europe（PEACE）を先日完成させました。このケーブルは、シンガポール、パキスタン、ケニア、エジプト、フランスなどを結びます。
- China Telecom は、先日、Asia Direct Cable の香港での陸揚げを完了させました。このケーブルは、中国本土、日本、フィリピン、シンガポール、タイ、ベトナムを結ぶ予定です。
- China Mobile は、2Africa ケーブルプロジェクトを所有する世界規模の企業連合に参加しています。2023 年から 2024 年にかけて完成予定のこのケーブルは、アフリカ、アジア、ヨーロッパの 33 か国にある 46 の陸揚局を接続します。
- China Mobile は Southeast Asia-Japan Cable 2 の所有権の一部を持つ予定です。このケーブルは 2024 年に敷設され、中国本土、日本、韓国、シンガポール、台湾、タイ、ベトナムを接続します。
- China Telecom は Asia Link Cable の所有権の一部を持つ予定です。このケーブルは 2025 年に敷設され、中国本土、ブルネイ、カンボジア、フィリピン、シンガポール、ベトナムを接続します。

ハイパースケーラーの台頭

海底ケーブル業界では、所有と運用の面で中国が目立った存在となるなか、民間セクターでも新しい重要なプレイヤーが現れました。以前のケーブルのエコシステムでは、AT&T のような大手通信プロバイダーが重要な存在となっていて、民間企業に帯域幅を販売していました。2010 年に Google が Unity-EAC Pacific ケーブルシステムに投資を行い、所有権の一部を保有するようになってから、Amazon、Meta、Microsoft なども含むハイパースケーラーが世界のケーブルネットワークの発展において主導的な役割を担うようになり、2015 年ごろからその傾向が加速しています。ハイパースケーラーは、ケーブルがどこを通り、どの国に接続するかを決めるようになっています。

従来の通信プロバイダーは、人口の多い地域のエンドポイントにいるユーザーを接続することを目的としていますが、ハイパースケーラーはデータセンター同士を接続することを目指しており、データセンターの多くは、経済的に理に適った、人口の少ない場所にあります。そのアプローチを実証する例としては、Google が最近完成させたケーブル、Equiano と Firmina は、南米とアフリカの拠点を結んでいます。これらのケーブルは、その拠点から陸上データネットワークを供給するために使われ、地域にインターネット接続を提供します。

Meta と Google は、自身で所有するか他のエンティティと共同で所有する海底ケーブルシステムを急速に増やしており、現在ではそれぞれの所有数は 16 と 21 となっています。Microsoft と Amazon は合わせて 6 以上のケーブルの所有権を持っています。現在稼働中の 529 のケーブルシステムのうち、ハイパースケーラーが所有権を持っているのは約 8%です。この割合は比較的小さいようにも見えますが、増加のペースは加速しています。2018 年から 2022 年にかけて敷設された 102 の海底ケーブルシステムでは、ハイパースケーラーは約 22.5%のシステムで所有権を持っています（**図 5**）。この傾向は単純な原因から生じています。それは、データの使用量が急増するなかで、直接の所有権を持つことの費用対効果が高まっているということです。ケーブル全体を対象としたデータキャパシティのシェアでは、2012 年から 2022 年にかけて、ハイパースケーラーのシェアは

約 10%から 71%へと増加しました。このように規模を拡大したことで、ハイパースケーラーは、ビジネスの要件に最も適したタイミングと場所でケーブルの接続を確立できるようになりました。

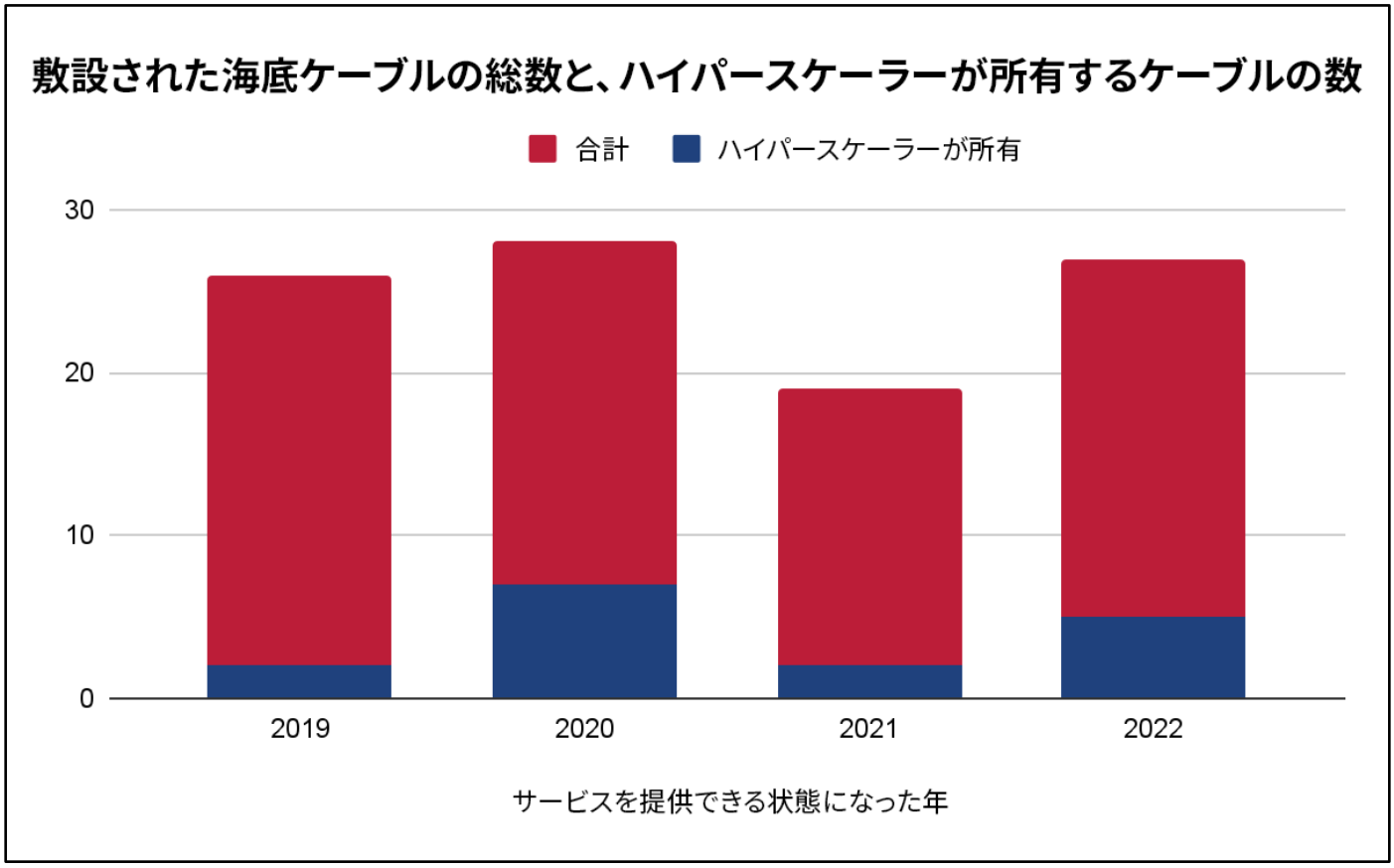


図 5：2018 年から 2022 年に、ハイパースケーラーが所有し、サービスを提供できる状態にあったケーブルシステム（出典：Recorded Future。TeleGeography のデータを視覚化）

歴史的に、ケーブルの所有構造としては、単一のエンティティが所有する場合が多くなっていました。ケーブルシステムの約 3 分の 2 は 1 つの企業によって所有されています。最近のデータでもこの傾向に変化はありません。2022 年に敷設された 22 のケーブルのうち 82%は単一のエンティティによって所有されていました。また、2023 年にサービスを提供できる状態になる予定の 36 のケーブルのうち 66%は単一のエンティティによって所有されます[4]。

単一のエンティティが所有するか複数のエンティティが所有するかによって、それぞれ独自の複雑さと制限があります。単一の所有者がいるシステムは、多くの場合、カバーする地域が狭かったり、ケーブルが短かったり、陸揚げされる場所の数が少なかったりします。フランス領ポリネシアの Natitua Sud や、アンゴラの各地をつなぐ Unitel North Submarine Cable などがこれに該当します。複数の所有者がいるシステムは多国籍企業連合によって管理されます。この形式では、より複雑なケーブルシステムの資金調達や運用が可能になります。前述の SEA-ME-WE 6 や 2Africa などがこれに該当します。企業連合モデルの短所は、関係者それぞれの優先事項や管理のためのアプローチの間でバランスを取る必要があることや、国有企業が関与してくる可能性があること、さまざまな政府による規制を遵守する必要があることなどです。

[4]これらの統計は、TeleGeography による海底ケーブルの地図についての Recorded Future による分析を反映しています。

これまでサービスが十分に提供されてこなかった市場向けのケーブルでは、ハイパースケーラーが主要な所有者や共同所有者になることが増えています。これは市場の独占やデジタル主権についての懸念をもたらします。ケーブルの所有者が強い力を持つことになり、これまでサービスが十分に提供されてこなかった市場において、政策面で考慮すべきこと、特にインターネットの規制やデータプライバシー関連の規制などに影響が生じます。Google と Meta は、それぞれアフリカと世界を結ぶ大規模なプロジェクトに着手しています。両社は、アフリカ大陸に送られてくる大量のデータのなかで、各自のプラットフォーム、つまり Facebook、Instagram、WhatsApp、YouTube などと、それらに関連するコンテンツを優先的に扱える技術力を持っています（また、そのような圧力を加える可能性があります）。そのことがアフリカの社会や政治体制に与える影響は非常に大きなものになる可能性があります。たとえば、アフリカの各国の政府は、ソーシャルメディアプラットフォームでコンテンツモデレーションを強化するように Google や Meta に迫ることが難しくなるかもしれません。アフリカ全体でソーシャルメディアプラットフォームを通じて虚偽の情報が流布されていることを考えると、これは重大な問題です。

物理的な攻撃と悪用に関する選択肢と課題

2022 年のロシアによるウクライナ侵攻、台湾統一を目指す中国による威圧的なアプローチの強まり、米中関係の悪化の継続など、最近の地政学的動向により、さまざまな国が、ケーブルシステムに物理的な攻撃をしかけて運用を中断させたり、ケーブルを流れるデータを国家安全保障や経済スパイの目的で秘密裏に入手したりする必要に迫られています。

海底ケーブルへの物理的攻撃

その目的、能力、影響を考慮すると、海底ケーブルに対する的を絞った物理的な攻撃を行う可能性が最も高いのは国家アクターです。できるだけ大きな混乱を引き起こして戦略的な目標を達成できる場所を特定したうえで、深海でケーブルを発見し、切断するには、専門的な知識と装備が必要です。それを持っている可能性が最も高いのは国家アクターです。国家アクター以外による技術的に単純な攻撃では、コストはかかるものの混乱は短期間で解決します。たとえば 2013 年には、エジプトのアレクサンドリア沖で、3 人のダイバーが SEA-ME-WE 4 海底ケーブルを切断しようとしたことがありました。しかし、国家アクター以外による攻撃は、海岸の近くで行われる可能性が高く、修復しやすくなります。2022 年には、フランスのマルセイユで未知の攻撃者によってケーブルが 2 回切断されましたが、破壊が行われたのが陸上だったため、ケーブルはすぐに修理されました。

図 6：マルセイユの陸揚局近くのマンホール内で破壊された海底ケーブル（出典：ソーシャルメディア）

ロシアが 2022 年 2 月にウクライナへの全面的な侵攻を開始し、中国は武力行使の可能性も含めて台湾統一に向けた準備を進めています。こうした事情により、海底ケーブルに対する地政学的な脅威が大きく変化し、ロシア政府と中国政府にとっては、海底ケーブルを不通にしたり破壊したりする動機が生まれています。海底ケーブルに対する物理的な攻撃を企てる可能性が現時点で最も高いのはロシアです。ハイブリッド戦争の戦略に従い、特に北海地域のケーブルが標的となる可能性があります。中国は台湾につながる海底ケーブルをすでに何度も破壊しています。台湾に侵攻することになれば、台湾付近の海底ケーブルはこれまでよりも中国による直接的な脅威にさらされることになるでしょう。ロシアと中国は、ステルス潜水艦、潜水艇、海上で活動できる民兵、深海のケーブルに到達できる特殊な水上艦などを展開できます。また、ケーブルを標的としたアクティビティと両国を結びつける明確な証拠があります。こうしたことから、両国は海底ケーブルにとっての脅威となると評価されています。

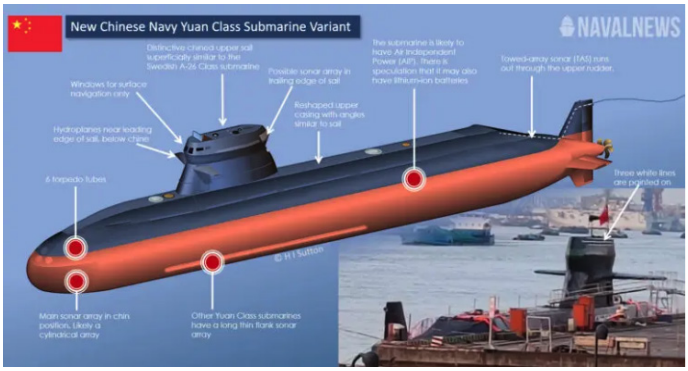
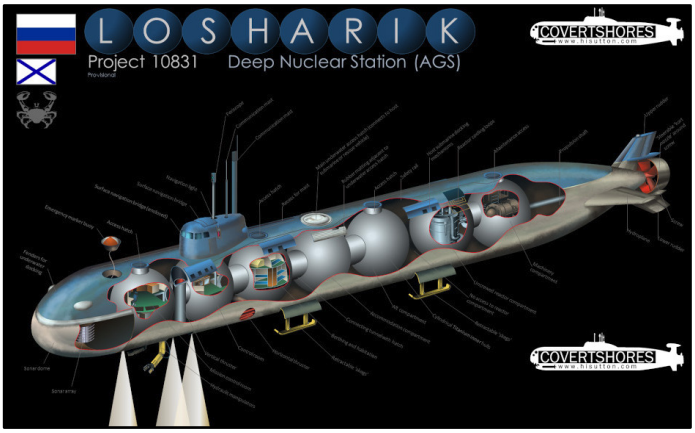
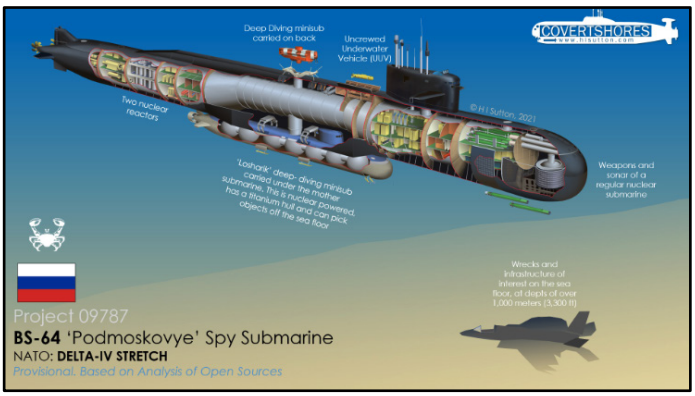
<table>
<tr><th colspan="2">中国</th></tr>
<tr><th colspan="2">現在運用中のステルス潜水艦/潜水艇/水上艇</th></tr>
<tr><td>● Type-039C
（出典：1、2、3）</td><td> 

図 7：中国の新しい潜水艦、Type-039C（出典：Naval News）</td></tr>
<tr><td>● 海上で活動できる民兵組織/民間の船団
（出典：1、2、3）</td><td> 
図 8：中国の民間の漁船（出典：Military Review）</td></tr>
<tr><th colspan="2">ケーブルの破壊との確実なつながり</th></tr>
<tr><td colspan="2">● 2023 年 2 月：台湾とその辺境の馬祖島を結ぶ 2 つの海底ケーブルが、6 日間のうちに中国の民間船によっておそらく故意に切断されました。台湾当局によると、台湾と周辺の島を結ぶケーブルは、2020 年以降、事故によるものと故意によるものを合計して 30 回にわたって破壊されています。</td></tr>
</table>

表 2：中国の能力の内訳と、海底ケーブルの破壊との確実なつながり
（出典：Recorded Future）

ロシア	
現在運用中のステルス潜水艦/潜水艇/水上艇	
● Belgorod（K-329） （出典：1、2）	 **図 9：**Belgorod K-329 潜水艦（出典：Naval News）
● Losharik（AS-31） （出典：1、2、3）	 **図 10：**Losharik AS-31 潜水艦（出典：Covert Shores）
● Podmoskovye（BS-64） （出典：1、2）	 **図 11：**Podmoskovye BS-64 潜水艦（出典：USNI News）

● Yantar （出典：1、2、3）	 **図 12：**Yantar 水上艇（出典：BBC）
ケーブルの破壊との確実なつながり	
● 2023 年 2 月：英国王立防衛安全保障研究所の所員の 1 人が、海底ケーブルなどのインフラストラクチャを標的とするための専用の潜水艦をロシアが開発している可能性が高いと主張しました。 ● 2023 年 2 月：オランダの軍情報保安局と総合情報保安局が共同で作成したレポートで、海底ケーブル、ガス管、集合型風力発電所などの北海沖のインフラストラクチャを破壊する準備をロシアが進めていると述べられました。 ● 2022 年 9 月：ノルドストリームのガスパイプラインが破壊される数日前に、デンマークのパトロール船がその付近でロシア海軍の艦艇を発見しました。その艦艇は水中での作戦用に設計された小型の潜水艇を運びます。 ● 2022 年 1 月：英国軍の国防参謀総長が、海底ケーブルは「世界の真の情報システム」であり、「ロシアは海底ケーブルを危険にさらす能力を拡大している」と述べました。 ● 2022 年 1 月：ノルウェー政府が、ノルウェー本土とスヴァールバル諸島を結ぶ海底ケーブルが切断されたことを明らかにしました。法執行機関の調査によると、そのケーブルは「人間のしわざ」によって切断されていました。	

表 3：ロシアの能力の内訳と、海底ケーブルの破壊との確実なつながり
（出典：Recorded Future）

海底ケーブルが破損するか完全に切断され、データを送信できなくなる障害は 1 年あたり平均で 100 件以上発生します。ケーブルの物理的破損の大半は事故によるものです。漁船の底引き網や、船舶が海底で錨を引きずったことが原因の破損が多く見られます。地質的なイベントによる破損の頻度ははるかに低いものの、その影響はより深刻になる可能性があります。2022 年 1 月には、トンガの沖で火山が噴火し、トンガで使われていた 2 つのケーブルに多数の障害が発生しました。その結果、1 か月以上にわたりインターネットにほとんどアクセスできなくなりました。

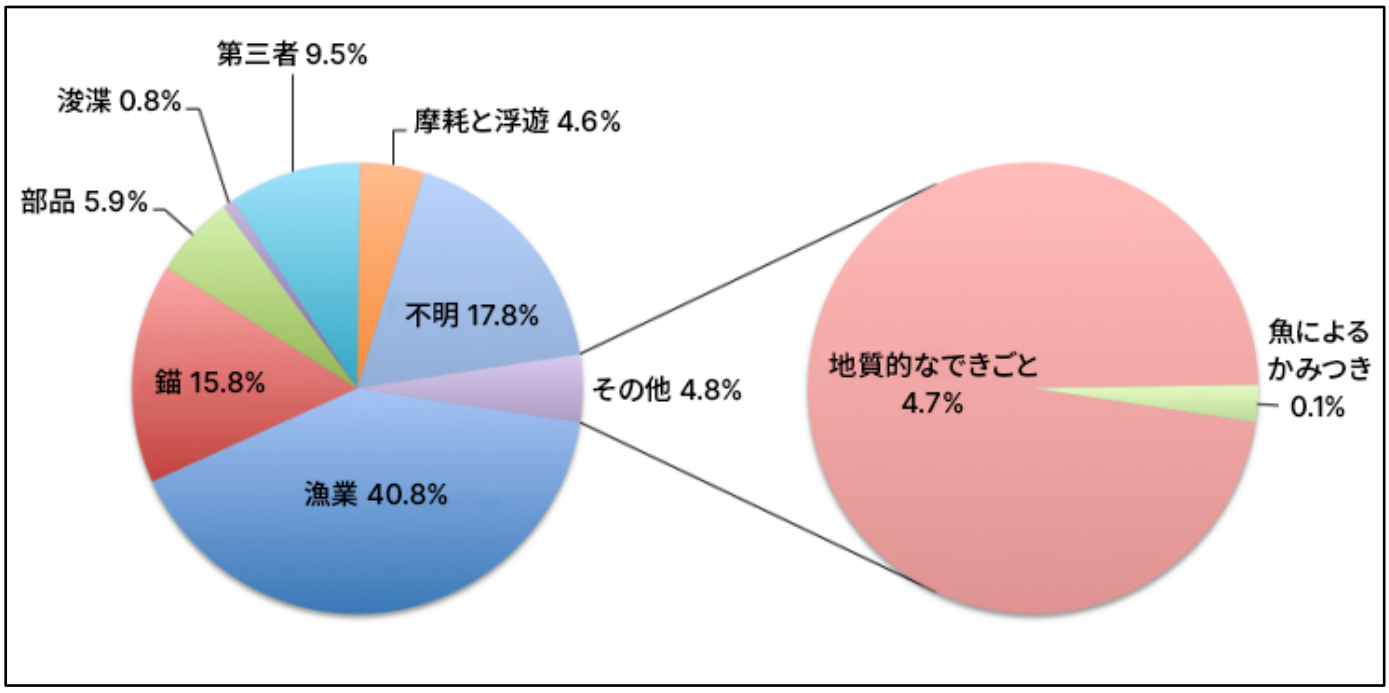


図 13：1959 年から 2021 年にかけて発生したケーブルの障害の原因（出典：International Cable Protection Committee）

頻度は低いものの、意図的な破壊はユニークな脅威ベクターとなっています。攻撃のタイミングと標的によっては、そのケーブルシステムを利用する国家や企業に対して非常に大きな影響を与えることができるからです。たとえば、トンガはインターネット接続を 1 つの光ファイバーに依存していたため、インターネット接続の面で壊滅的な打撃を被ることになりました。別の例としては、台湾とその辺境の馬祖島を結ぶ海底ケーブルは過去 5 年で何度も切断されており、意図的な攻撃が疑われますが、こちらの影響はそこまで大きくなく、インターネット接続が遅くなり、電話がつながりにくくなる程度で済んでいます。しかしそこから得られる教訓は明確です。海底のデータライフラインは攻撃者が選択したタイミングと場所で混乱にさらされやすいものであるということがわかります。

海底ケーブルに対して物理的な攻撃を意図的に行うのは、最近始まったことではありません。米西戦争の最中、1898 年には、フィリピンのマニラと香港を結ぶケーブルを USS Zafiro が切断し、そこに拠点を置いていたスペイン軍の情報のやり取りを困難にしました。それから 20 年と経たない第一次世界大戦の初期には、英国が浚渫を行ってドイツの電信ケーブルを破壊し、ドイツの通信能力を奪いました。より最近の 2015 年には、米国の国家安全保障の関係者が、北海と北東アジアを結ぶケーブルの近くで作戦行動を取るロシアの潜水艦と、アメリカ大陸の沿岸を運航するロシアの水上艇 *Yantar* がもたらす物理的な脅威について警告を発しました。2017 年には、ノルウェーの海底潜水艦監視ネットワークの接続に用いられていた 2.5 マイル（約 4km）のケーブルを未知のアクターが切断し、取り除きました。そのネットワークを所有し、運用していたノルウェー海洋研究所以外に与える影響は比較的わずかでしたが、潜水艦が北部の重要な航路を検知されずに通りやすくなりました。

海底ケーブルを通じて伝送されるデータの量は増加し、その機密性は高まっています。海底ケーブルは世界中の金融において中心的な役割を果たすようになっているため、物理的な攻撃が行われた場合の影響が大きくなっています。さまざまなプロバイダーや業界でクラウドコンピューティングの導入が進み、その顧客も含めて、低遅延で高品質のソリューションへの依存が強まっています。5G の発展と普及は、特にアフリカにおいてこの依存傾向をさらに強化するでしょう。

超高速通信網への侵入

海底ケーブルは、治安の強化や経済的な優位性の獲得のためにインサイトを収集したい国家にとって有益な情報源となります。水中でのインテリジェンス収集には長い歴史があります。特に有名なのは冷戦時代に米国が実行した作戦、アイヴィー・ベルです。この作戦では、オホーツク海にあったソ連の重要な軍事通信用ケーブルから米国が情報を入手しました。海底ケーブルシステムが急速に拡大し、水中の超高速通信網に侵入する機会が増加しています。ケーブルが岸に着くところである陸揚局が最も脆弱な標的となる可能性が高いと考えられます。

アイヴィー・ベルを今日に再現するうえで問題となるのは、海底ケーブルを流れるデータの規模が最大で毎秒 250 テラバイトと莫大であることです。水中からデータをフィルターして、陸上のアナリストに送る仕組みを確立する必要があり、これは極めて困難であると言われています。深海にあるケーブルを悪用できれば活動は検知されづらくなりますが、それが可能な国はごく少数に限られると考えられます。陸揚局は海底のケーブルよりもアクセスしやすい標的です。

陸揚局は、海底ケーブルのエコシステムにおいて重要なものであるにもかかわらず、特にセキュリティが強化されていない平凡な建物であることが多く、通信事業者、データセンター、ポイントオブプレゼンス（PoP）に近い場所という理由で選ばれています。施設を運営するのは、地域の通信事業者、海底ケーブルの所有者、あるいは国際的な企業連合です。先進国であっても施設のセキュリティの程度はさまざまです。たとえば、シエラレオネのフリータウン郊外にある Africa Coast to Europe ケーブルの陸揚局は、塀で囲まれた狭い土地で、近隣の区域から離れていません。

図 14：シエラレオネのフリータウン郊外にある陸揚局
（Planet の SkySat の画像。解像度は 50cm。SkyWatch 提供）

岸の近くではケーブルへのアクセスが十分に保護されているとはかぎりません。複数のケーブルが似た経路を通るようにする慣習によって事態は悪化し、重大な要衝が作り出されています。たとえば、2022 年にはマルセイユでケーブルが切断されるインシデントが発生しました。マルセイユには現在陸揚げされているか近い将来陸揚げされる予定のケーブルが 16 あります。国家アクターによるインテリジェンス収集作戦では、このようなセキュリティの弱いアクセスポイントが悪用される可能性が高いでしょう。場合によっては、侵害したケーブルにデータを流すための物理的攻撃を行う可能性もあります。

陸揚局は、その所有者によって監視機器やバックドアソフトウェアが追加され、所有者が所属する国家あるいは外国政府のためのインテリジェンス収集拠点として使われる可能性があります。陸揚局を標的とするインテリジェンス収集作戦のリスクを示す最近の例を 3 つ挙げます。

- Baie Jacotet の陸揚局にインターネットの「スニッフィング」機能の追加を許可するよう、インドの情報機関に代わってモーリシャスの首相が Mauritius Telecom に圧力をかけた疑いが生じ、このモーリシャス政府の行動が物議を醸しています。
- 退任を控えたミクロネシア連邦のデイヴィッド・パヌエロ大統領は、先日公開した書簡で、ミクロネシア連邦の海底ケーブルと通信インフラストラクチャを中国政府が管理することを許可する合意覚書に署名するよう、中国が何度も要求してきたと主張しました。
- 2021 年に、米国政府の諸機関で構成される委員会は、キューバ国内で ARCOS-1 ケーブルシステムの新しい陸揚局を作成することを目的としたライセンス申請を拒否するよう提言しました。その理由として、キューバの国有通信会社、Empresa de Telecomunicaciones de Cuba S.A.（ETECSA）が関与しており、スパイ活動が行われる懸念があることを挙げました。

海底ケーブルに対するスパイ行為への防御策としては、依然として暗号化が有力です。脅威アクターがデータを悪用する能力を制限できる可能性は高いと考えられます。量子コンピューターが発展し、まもなく暗号を解読できるようになるのではないかという懸念がありますが、最近の研究から、量子コンピューターは効果的な防御を維持するためのツールともなり得ることがわかっています。2019 年に、研究者が量子鍵配送のテストに成功しました。このテストでは、長さ 96 キロメートルにおよぶ海底ケーブルで、量子もつれ状態にある光子のペアを使って通信を保護できました。2020 年には、Microsoft がポスト量子暗号を使用して、水中のデータセンターと接続するネットワークトンネルを暗号化し、保護しました。

ネットワークの管理の脆弱性

コストの削減、運用の効率化、パフォーマンスの向上のために、海底ケーブルの所有者と運営事業者は、インフラストラクチャを監視および制御するリモートネットワーク管理システムの利用を進めています。リモートネットワーク管理システムを利用するにはインターネットへの常時接続が必要であるため、国家支援型の攻撃者、ランサムウェアグループ、ハクティビスト、その他のサイバー脅威アクターによる攻撃にさらされることになります。このように、利便性を追求すると大きなコストが生じる可能性があります。サードパーティの脆弱性がケーブルシステム全体のセキュリティと耐障害性を危険にさらすことになるからです。2022 年 4 月にはそうした未来が現実になりかけました。米国の当局は、ハワイで使われていた海底ケーブルの運用システムに対するサイバー攻撃を阻止しました。その攻撃はサードパーティのクレデンシャル関連の侵害によって可能になったものでした。

以前は、海底ケーブル用の端局装置と給電装置の管理には、現場にあるシステム監視ツールが使われていました。発展した技術を取り込むなかでケーブルシステムが複雑化し、Ciena や NEC Corporation が提供するリモートネットワーク管理システムが導入されるようになりました。1948 年にクロード・シャノンが発表した定理によると、エラーを発生させずに通信路を介してデータを送信できる最大の速度が存在します。その速度はシャノン限界と呼ばれています。通信速度がシャノン限界に近付くなかで、データフローの効率を改善して帯域幅を向上させることの重要性が高まっています。新しいネットワーク管理システムを使うと、データフローの効率を改善するために、運用者は海底ケーブルシステムの事実上あらゆる要素を制御できます。「他国にあるものも含めて、物理的な光学のレイヤー、端局装置、中継器、分岐装置、陸揚局、その他のネットワーク運用センター」を制御できます[5]。ベンダーの新しい製品は、オープンな API を使用するクラウドネイティブプラットフォームであり、外国にあるケーブルのシステムとサードパーティのインターネットインフラストラクチャを視覚化できることを売りにしています。

リモートネットワーク管理システムは、コストの削減とパフォーマンスの向上を可能にしますが、一方で、リスクが増加してコストがかかる可能性があります。リモートネットワーク管理システムを利用するには、ケーブル、オープンソースのソフトウェア、Windows や Linux などの OS がインターネットに接続する必要がありますが、サイバー脅威アクターはこれらのソフトウェアや OS を悪用する方法を熟知しています（1、2）。リモート管理システムや同様の製品の脆弱性を悪用した近年のサイバー攻撃で大規模なものとしては、2020 年に SolarWinds の Orion プラットフォームが侵害された例や、2021 年に Kaseya の製品である Virtual Systems Administrator が

[5]Michael Sechrist 氏、“New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems” p. 12.Belfer Center Discussion Paper、No. 2012-03、Harvard Kennedy School、2012 年 2 月

侵害された例などがあります。これらの攻撃は、サードパーティを利用することに伴うリスクを示しています。侵害された製品が顧客のネットワークで特別な権限を持っている場合は特にリスクが高くなります。

今後の展望

デジタル化した今日の世界において、データが血液だとしたら、海底ケーブルはそれを支える重要な血管です。海底ケーブルの代わりになりそうなものは見つかっていません。データへの需要が高まり続けるなかで、世界の金融、国家の安全保障、国際的な通信における海底ケーブルの重要性は確実に向上するでしょう。海底ケーブルネットワークは拡大し続け、ハイパースケーラーが台頭し、ネットワーク管理システムを用いた効率の最大化を目指す取り組みが行われています。こうした動向から、データに対する需要は満たされる可能性が高いと考えられますが、同時に、複雑さが増し、脅威アクターによる悪用の機会も増加するでしょう。

ロシアがウクライナに侵攻し、中国が台湾との統一に備えて威圧的な言動をとり、米中関係が悪化しているため、海底ケーブルの所有者と運営者、海底ケーブルを利用する国家と企業にとっての地政学的なリスクの環境は短期的には悪化する可能性が高いと考えられます。国家支援型の物理的な攻撃やサイバー攻撃のリスクが向上するでしょう。こうした攻撃の影響はさまざまで、トラフィックが断続的に途切れる程度で済むこともあれば、復旧まで数日から数週間かかるような大規模な障害につながることもあるでしょう。損害の程度は影響を受けるネットワークの冗長性と耐障害性によって異なります。

エッジでのスパイ活動を目論む国家アクターは、インテリジェンス収集のために海底ケーブルのエコシステム全体を標的にするでしょう。陸揚局のインフラストラクチャ、海底ケーブル自体、サードパーティのプロバイダー、そしてすべてを結ぶハードウェアとソフトウェアが標的となります。それとは別に、ロシアは海底ケーブルの地図の作成を目に見える形でもそうでない形でも進めるでしょう。また、陸上と水中の両方で的を絞った破壊を行う可能性が高いと考えられます。これは、西側諸国に不都合を強いるためであるとともに、ハイブリッド戦争の応用例の有効性を見極めるためでもあります。中国も、台湾が利用するケーブルに対して、引き続き調査と破壊を行う可能性が高いと考えられます。

ハクティビストやランサムウェアグループなど、国家以外のアクターは比較的能力が乏しいと予想され、海底ケーブルのネットワークや運用システムに脅威をもたらす可能性は低いと考えられますが、そのリスクは軽視できません。船の錨や漁船によって偶発的な損害が生じることは引き続きよくあると思われますが、その影響は大きなものにはならないでしょう。

Insikt Group®について

Insikt Group は Recorded Future の脅威調査部門です。政府、法執行機関、軍、情報機関での豊富な経験を持つアナリストとセキュリティ研究者が在籍しています。そのミッションは、幅広いサイバー脅威と地政学的脅威についてのインテリジェンスをもたらして、お客様のリスクを軽減し、具体的な成果を上げ、ビジネスの中断を防ぐことです。国家支援型の脅威グループ、ダークネットや犯罪者が集まるアンダーグラウンドで金銭を目的として活動する脅威アクター、新しいマルウェアと攻撃者のインフラストラクチャ、戦略地政学、影響工作などについて調査しています。

Recorded Future®について

Recorded Future は世界最大級のインテリジェンス企業です。Recorded Future のクラウドベースのインテリジェンスプラットフォームは、攻撃者、インフラストラクチャ、標的を包括的にカバーしています。Recorded Future は、継続的かつ広範な自動でのデータ収集および分析と人による分析を組み合わせることで、広大なデジタル空間をリアルタイムで可視化し、お客様が事前対策により攻撃を阻止して、人、システム、インフラストラクチャを保護できるよう支援します。ボストンに本社を置き、世界中にオフィスと従業員を展開しており、60 か国以上の 1,500 を超える企業と政府系機関で利用されています。

詳しくは、recordedfuture.com をご覧ください。また、Twitter で@RecordedFuture をフォローしてください。