

CIRCULAR

Ref: 01/22 2022年2月

アウトライン

- 2010年以降、世界貿易の90%が海上輸送によるものであることを反映して、数多くの制裁措置が海運業とその関連産業に向けられてきました。
- 本回覧の目的は、各国政府や国連などの国際機関による制裁体制に違反する活動を行う集団が用いている最近の偽装取引の手口について、メンバーの皆様にご注意喚起を行うことです。
- 制裁違反に使われる偽装行為の手法には、数年前から使われてきたものもありますが、過去18か月で使われるようになった新しい手口が次第に広まったものがあります。
- コンプライアンス体制を適切に取入れることは、不注意に制裁違反に関与することを、回避するのに役立ちます。

メンバー各位、

制裁 - 最近の偽装行為による取引手法

はじめに

2010年以降、世界貿易の90%が海上輸送によるものであることを反映して、数多くの制裁措置が海運業とその関連産業に向けられてきました。

本回覧の目的は、各国政府や国連などの国際機関による制裁体制に違反する活動を行う集団が用いている、最近の偽装取引の手口について、メンバーの皆様にご注意喚起を行うことです。

国際グループ等が確認している最近の偽装行為

貿易制裁は、各国政府の外交目的を推進するため広く採用されていますが、以下の国・地域については、海上貿易活動の規制という観点から、特に注意が必要です。

- イラン
- シリア
- ベネズエラ
- 朝鮮民主主義人民共和国 (DPRK)
- クリミア
- キューバ
- ベラルーシ

国際的および国内の制裁措置に違反して取引される貨物は、増加傾向がみられます。イランからの石油輸出は当初、制裁措置で厳しく制限されていたにもかかわらず、米国の JCPOA から撤退した後は、1日あたり推定 34 万バレルであったものが、2021年3月には1日あたり推定 130 万バレルにまで増加したと言われています¹。

¹ 米国議会調査局レポート “Iran Sanctions RS20871” <https://crsreports.congress.gov>

ここ数週間、イランとベネズエラのアジア市場に向けた石油貨物のスワップ取引についてのニュースが、マスコミで広く報道されました²。2021年9月には、国連安全保障理事会の北朝鮮専門家パネルが、海運業および北朝鮮が関与する国連制裁への広範な違反行為について詳述した中間報告書を発表しました。報告書はこちらのリンクよりご覧いただけます。
[S_2021_777_E.pdf\(securitycouncilreport.org\)](https://www.securitycouncilreport.org/S_2021_777_E.pdf)

制裁違反に使われる偽装行為の手法には、数年前から使われてきたものもありますが、過去18か月で使われるようになった新しい手口が次第に広まったものがあります。偽装の手口はいずれも、船舶や貨物、地理的位置、航行活動の特定を妨げ、隠蔽することで、監視や探知から逃れることを目的としています。これらの手口により、船主やその取引相手は、制裁に違反する貨物を輸送していると気づかず、利用されてしまうリスクがあります。

偽装の手口には以下のような行為が含まれます。

- 船舶の自動識別信号(AIS)を操作して、船舶の位置を偽装したり、船舶のデジタルIDを変更する。
- 船舶の外観を変更する。
- 船舶・貨物に関する文書を改ざんする。
- 制裁対象国からの貨物であることを隠すため、複数回にわたり船舶間の貨物移動を繰り返す。

制裁回避を防ぐためのコンプライアンス体制を適切に取り入れていない船主には、制裁対象の貨物輸送に船舶が利用されてしまうリスクが発生します。

船舶の自動識別信号(AIS)の操作

国連の報告書や米国、英国の海事ガイダンス³では、適切なコンプライアンス体制の一部として、船舶のAIS信号の送受信を監視する必要性を特に強調しています。

ただし、AISの技術やその関連ハード・ソフトウェアの本来の目的は、監視することではなく、沿岸水域の船舶を特定し、衝突リスクを回避することにあります。AISの機能は安全促進を目的としており、送信される信号が故意に操作されることを防ぐような設計にはなっていません。また船舶の安全とセキュリティのためであれば、信号の送信を停止することは依然として合法になっています⁴。

AIS信号は操作したり停止したりすることができるので、制裁回避に悪用されやすいと言えるでしょう。AISには、偽造データ送信を防ぐセキュリティ機能が内蔵されているものの、その機能はメーカーによってまちまちであり、またセキュリティ機能を停止することもできます。機種によりますが、AISのエンコード内容はパスワードを使って変更できるようになっていますが、そのパスワードが常に厳重に保護されているわけではありません。

AISに直接手を加えた上、さらに複数のAISを導入し、1隻の船舶から複数のAIS信号を送信し、船舶の身元や位置を偽装することも可能です。船舶の識別情報を改ざんし、船舶を外観からも、デジタルの面からも偽装する手法は、よりいっそう一般的になってきています。

² 2021年9月25日付 ロイター通信記事「米国の制裁下で、イランとベネズエラが石油輸出契約を締結」

³ 米国務省、財務省外国資産管理局(OFAC)と沿岸警備隊(USCG)は、関連業界のデューデリジェンス体制を支援するため、2020年5月に発表したGlobal Maritime Sanctions Advisoryで、船主、旗国、船級協会、銀行、保険会社を含む海運関連業界にコンプライアンスに関する指針を示しています。また英国金融制裁推進局(OFSI)も同年7月に、英国の海運業界に従事する事業者や個人のコンプライアンスへの理解が深まるよう、Maritime Guidanceを発表しました。いずれのガイダンスも、包括的な制裁遵守プログラムを企業の実務に適切に組み込むことの重要性を強調しています。

⁴ 1974年の海上人命安全条約(SOLAS)の規則V/19では、国際航海に従事する300総トン以上のすべての船舶、国際航海に従事しない500総トン以上の貨物船、大きさにかかわらず客船について、規則V/19.2.4で規定された船舶自動識別装置(AIS)を装備することが義務付けられています。AISを解除できる状況については、IMO決議A.917(22)の paragraph 21をご参照ください。SOLAS規則V/34-1では「船主、用船者、規則IX/1に定義される船舶運航会社、またはその他の者は、船長が専門的判断により、海上の人命の安全及び海洋環境の保護に必要な決定を行うことまたは決定を実行することを妨げたり制限したりしてはならない。」と規定しています。

AIS を利用した偽装の手口は以下の行為を含みます。

1. AIS の電源を切る

AIS の電源を切るとは、特定の状況下においては SOLAS 条約で許可されていますが、制裁を回避しようとする船舶は、船舶の位置や動向を隠すために AIS の電源を切ることがあります。あまり高度な技術を持たない制裁違反者には、この手法は依然として一般的で、彼らは船長が AIS の電源を切ることには正当な理由がある、とか適切に信号を送信しても受信されないこともあるなどと言い訳をするケースが未だに見られます。

したがって、STS(船舶間貨物移送)を行うメンバーは、貨物移送の相手船の AIS 送信履歴に空白期間がないかどうかを監視することを推奨します。相手船を監視するために、民間企業が提供している AIS 監視プラットフォームやサービスを利用することもご検討ください。こういったサービスでは、AIS 信号送信の空白期間に違法行為が行われていたかどうかを検証するための技術やアルゴリズムが使われています。

単純なケースとして、例えばオマーン湾に入る際に AIS の電源を切り、制裁対象の貨物を積載または STS の後、再び AIS の電源を入れることによって、制裁を回避しようとするところがあるかもしれません。より巧妙な手口として、AIS の電源を切る前に、船舶の本来の航路を偽装するため、わざと違う航路を捏造することもあるでしょう。

2. GPS/GNSS の操作(位置情報の偽造)

実際の船舶の位置を偽装するため、船舶が AIS から発信する位置情報を改ざんする制裁違反者もいます。

GPS や GNSS(全球測位衛星システム)による、位置情報の偽装手法のうち最も初歩的なものは、同じ位置での AIS の送信履歴更新を単純に繰り返すことです。より巧妙な手法としては、衛星画像や実際の船舶の目視、または合成開口レーダー(SAR)の記録等と照合しない限り判別不可で、まるで本物のように見える信号を捏造するというものもあります。国際 P&I グループ(IG)は、GPS/GNSS の操作によって、制裁違反を行っている船舶の実際の位置情報を隠蔽する事例が増加していることを重く見ています。

船舶の実際の位置情報であることを証明するために必要なデータ類を検証できる AIS 監視プラットフォームの専門業者との契約を検討されるのも良いでしょう。

3. AIS と識別情報の悪用

AIS 送信が、他の船舶の識別情報を複製し悪用するために事例がますます増加しています。船舶は、他の船舶によって既に使われている MMSI 番号(海上移動業務識別コード)を送信することがあります。複数の船舶が MMSI 番号を使って通信しているため、制裁違反を行っている船舶は、AIS の更新によって生じるノイズに隠れることができます。また、他の船舶の識別情報を複製する際(「ゴースト」や「ツイン」などと呼ばれる)、制裁対象ではない船舶の識別情報を得られた場合は、それを悪用することもあります。

識別情報を複製され悪用された船舶には、無作為に選ばれた無実の船舶の場合もあれば、制裁違反船と前もって打ち合わせた場所で自身の識別情報を引き渡し、その後制裁違反船が AIS を再開するという形で制裁違反に共謀している船舶もあるでしょう。

識別情報の改ざん

船舶の識別情報を偽装するために、制裁違反者によって用いられる手法はますます巧妙になっています。

1. 船舶の外観を変更

衛星画像やその他の監視技術は、制裁違反船舶を特定するために民間や軍の監視者によって使用されています。制裁違反者は、自動分析を妨害するために、甲板や船体の色といった船舶の外観を変える事例が今後ますます増えていくでしょう。また、船舶を特定する上でキーとなるような、外観の特徴的な部分が防水シートで覆われ隠されることがあるかもしれません。

2. 船舶の識別情報の物理的な変更

最近の多くの出版物⁵によると、船体の横に表示されている船名や IMO 番号が書き換えられた事例を紹介しています。AIS 信号が、全ての関連書類と同様に偽の識別情報が使用される例もあります。

3. 船舶の登録番号の変更

IMO に新たに登録されたと思われるような偽の識別番号を、あたかも「クリーン」な識別番号として取引を試みた事例も報告されています。

虚偽の書類

貨物の原産地について関係者や各国を欺くため、船舶や貨物に関する虚偽の書類を作成する手法が、しばしば AIS の不正操作と組み合わせて使われます。虚偽の貨物書類には、虚偽の貨物の原産地や特性が記載され、制裁違反を行う船舶についても偽りの船名や識別情報が記載されます。

虚偽の識別情報の一部として、偽の船籍が記載されることがあります。制裁回避のために有利な旗国が利用されます。具体的には、容易に連絡を取る手段がなく、詳細を確認することが困難な旗国で、虚偽の旗国登録のうちいくつかは実在しておらず、または外国籍船を受け付けていない可能性があります。また、短期間のうちに、いわゆる「フラッグホッピング」と呼ばれる、頻繁に船籍を変える船舶にも注意する必要があります。

また、船舶の運航に制裁対象者が関与していることを隠蔽するために、実態のないペーパーカンパニーや、所有・管理を複数のレベルで行うような、複雑なビジネス構造を利用する手法も見られます。船舶の所有者や管理者を頻繁に変更しているケースには、注意が必要です。船舶の購入後、高リスク地域からの 1 航海のみを行い、その直後に新しい所有者に船舶を譲渡することを繰り返す事例が確認されており、船舶の運航に組織的な制裁違反取引を行う者が関与している可能性があります。

書類が虚偽であることを証明するのは非常に困難で、例えば、貨物を積載したとされている期間に実際に寄港していたかを港湾のリストで確認するなど、複数の情報源をチェックして実証する必要があります。メンバーは、当該港の信頼できる現地代理店に確認するとよいでしょう。

船舶間貨物移送(STS)

貨物の本当の産地を偽装するために STS が利用されることがあり、事情を知らない船主にとって大きなリスクとなっています。貨物を複数回にわたり船から船へ積み替え、他の貨物と混載し、虚偽または一部虚偽を含む書類と組み合わせることにより、本当の貨物特性を特定することは極めて困難になります。

より巧みな制裁違反者は、衛星画像データの収集タイミングを知っており、違法な STS を計画する際にこれを考慮に入っていたという事例も、IG 加盟クラブに報告されています。

違法貨物の原産地をごまかすために、STS が合法的に行われている海域で STS を行うことで、虚偽記載された貨物の内容と一致させるという手法もあります。例えば、ペルシャ湾や東アジア海域で STS を行うことで、イラン産の石油をイラク原産と偽装することがありますが、これはイラク産石油の取引がよく行われている海域であるからです。

STS オペレーションは、各船舶ごとに考えるべきではありません。合法的な STS であっても、相手船が以前に制裁貨物を輸送した船舶と STS を行っていた場合には、制裁の対象となる可能性があります。

⁵ 国連安全保障理事会 北朝鮮専門家パネル 中間報告書 S/2021/777 “Unmasked. Vessel Identity Laundering and North Korea’s Maritime Sanctions Evasion” C4ADS 2021

制裁逃れの結果

多くの制裁関連法は、船主やその他当事者が、制裁違反が発生する前に、相当の注意義務を尽くしていたかどうかを問題にします。しかし実際には、船主がその制裁体制の下で違法とされる貨物を輸送していたと発覚した場合、船主のコンプライアンス対応や事情を酌量せず、船主に対して厳しい措置が取られることが通例です。各国は、制裁違反者がその対象となる刑事司法制度を通じて、または制裁違反者が国外で居住している場合は、制裁対象者として記載された指定・制裁対象リストによってのみ、制裁を執行することができます。制裁対象者として指定されると、銀行、用船者、保険会社など第三者がその船舶所有者と取引することは違法とされることになります。

制裁違反行為に関係したことが報道等により公にされると、非常に大きなダメージとなる可能性があります。IG は、根拠が無いかかわらず制裁違反の嫌疑をかけられた船舶が、入港や銀行取引を拒否されたり、船籍登録を抹消されたりする事例を確認しています。

当クラブの保険カバーは、違法取引に対しては適用されません。また、取引自体は合法であったとしても、保険を提供することによって当クラブがリスクにさらされたり、制裁に違反したりする可能性があると判断された場合には、保険契約が解除されることがあります。

詳細について、米国の Maritime Advisory ([05142020_global_advisory_v1.pdf](#) (treasury.gov))や英国 OFSI の海事ガイダンス([OFSI_Guidance_-_Maritime_.pdf](#) (publishing.service.gov.uk)) をご参照ください。不注意や認識不足によって制裁違反の疑いをかけられるリスクを最小限に抑えるため、AIS ソフトウェアの専門業者との契約を検討されてもよいかもしれません。

国際グループのすべてのクラブは同様の回覧を発行しています⁶。

UKP&I クラブ 日本支店

⁶ IG は本回覧の発行にあたり、技術的助言をいただきました Geollect Limited ([www.geollect.com](#))に感謝いたします。