SHIP SECURITY ADVISORY No. 08-26J

To: **Owners/Operators, Masters, Company Security Officers, Recognized Security Organizations**

SUBJECT: **MARITIME CYBER SECURITY: TARGETING OF SHIPBOARD NETWORK INFRASTRUCTURE**

Date: **30 October 2026**

悪意あるサイバー攻撃者による商船への攻撃が増加していることについての注意喚起となります。

船内のインターネット接続可能なネットワーク機器やシステムが、船舶の情報技術 (IT) システムおよび運用技術 (OT) システムへの侵入経路として悪用されています。

1.0 概要

1.1 本通知書は、2026年8月に米国向け航海中の商船に対して実際に実施された法執行機関およびポートステートコントロールの措置、ならびに同時期に船主および運航者が外国の法執行機関およびコンピュータセキュリティインシデント対応当局から受領した通知を受けて発行しています。

2.0 背景

2.1 米国沿岸警備隊 (USCG) および連邦捜査局 (FBI) は、2026年8月中に米国向け航行中の2隻の船舶がサイバー攻撃を受けた疑いがあることを確認した。そのうち1隻は、船舶のネットワークが外国のサイバー主体によって侵害された兆候が確認されたことを受け、2026年8月21日にメキシコ湾において、米国沿岸警備隊の法執行担当者、船舶検査官、サイバー防護要員、およびFBIのサイバーチームから成る合同チームによる立入検査を受けた。もう1隻についても、2026年8月24日に立入検査が実施された。[1]

2.2 1隻目の船舶は、侵害を受けた時点でジブラルタル海峡を航行中であったと報告されており、30時間を超える期間にわたり通信を喪失したとされている。当局は、この事案による運航上の支障、船舶の安定性への影響、乗組員に対する身体的危険、または環境への影響は確認されていないと報告している。

---

1 ABC News, Coast Guard, FBI investigating after 2 oil tankers bound for US hit with cyberattacks: Sources, 16 September 2026; and CBS News, Coast Guard, FBI boarded Texas-bound commercial oil tanker to investigate cyberattack, 15 September 2026.

本船舶保安通知は、毎年弊局によって審査され、特段の記載が無い限り、また置き換え、取り消しが無い限り、発行・更新から1年後に失効します。

注）本和訳はご参照頂き易い様に用意されたものでマーシャルアイランド海事局発行の公式文書ではありません。本和訳とマーシャルアイランド海事局発行の公式英語版内容に齟齬が生じた場合は常に英語版を正とします。

2.3 これとは別に、また公開報道に基づくものではない情報として、国家警察当局が発した通知が、国家コンピュータ・セキュリティ・インシデント対応チームを経由して用船者へ伝達され、さらに船舶運航会社へ転送された事例があった。そのような通知の一例では、対象船舶が船名およびIMO番号によって特定され、当該船舶はサイバー侵害を受けていると明記されており、船内にインストールされたファイアウォール機器についても、その公開IPアドレスを示したうえで、当該機器に保存されているログを保全するよう要請していた。この種の通知は、海事当局から直接届くとは限らず、商業上のルートを通じて会社へ伝達される場合があり、港湾国当局からの連絡よりも先に届く可能性もある。

2.4 現時点では、いかなる国家または組織も本件への関与を表明しておらず、また、いずれの政府も公には攻撃主体の特定を行っていない。

3.0 評価

3.1 商船は、無差別的・偶発的なマルウェア感染ではなく、意図的なネットワーク攻撃の対象となる可能性がある。国家警察当局や国家インシデント対応機関が、特定の船舶名および特定の機器を名指しで識別して通知を行っているという事実は、船内での通常のアンチウイルス検知に基づくものではなく、情報機関や法執行機関による情報収集から得られた情報に基づく報告である可能性と整合している。

3.2 インターネットに接続されたネットワーク機器のうち、衛星通信システムとの接続境界に設置されるインフラ、主としてファイアウォール、ルーター、およびVPN装置が、最も侵入経路となる可能性が高い。 これらの機器は設計上インターネットからアクセス可能であり、多くの場合は第三者によって遠隔管理されている。また、ファームウェアの更新が数世代遅れていることが少なくなく、船内のワークステーションに導入されているアンチウイルスソフトウェアの保護対象外となっている。 USCGおよびFBIは別途、米国海上輸送システム (MTS: Marine Transportation System) に属する船舶および施設で使用されているFortinet FortiGate機器が、国家支援型サイバー攻撃グループによる悪用の対象となっていることを指摘している。また両機関は、FortiBleedとして知られる認証情報窃取キャンペーンにより、インターネットに公開されたFortiGateファイアウォールおよびSSL-VPNゲートウェイの管理者認証情報が大規模に漏えいしたと警告している。詳細については、以下を参照のこと ; USCGおよびFBI Maritime Cyber Alert 02-26 “Fortinet FortiGate Vulnerabilities”, FBIおよび米国シークレットサービスの勧告 JCSA-20261006-01。

3.3 侵害は、侵害発生からかなり時間が経過した後に、しかも本船の外部によって検知されている。したがって、船内で異常が検知されていないことをもって、侵害が発生していない証拠とみなすべきではない。

3.4 通信境界での侵害は、攻撃者に対し、航海情報、貨物情報、および乗組員情報を与える事になり、陸上との通信を妨害出来る事にもなる。ネットワーク分離が適切に行われていない場合には、航海支援システムや貨物運用システムにまでアクセスを拡大したりする可能性がある。
現時点での主なリスクは、情報の機密性、通信の可用性、ならびに商業上および港湾国当局に対する信用・評価への影響にある。一方で、ITネットワークとOTネットワークが分離されていない場合には、安全面にまで影響が及ぶ可能性がある。

注）本和訳はご参照頂き易い様に用意されたものでマーシャルアイランド海事局発行の公式文書ではありません。本和訳とマーシャルアイランド海事局発行の公式英語版内容に齟齬が生じた場合は常に英語版を正とします。

3.5 リスクは船内機器だけに限定されるものではない。 米国海事局 (MARAD) は、外国製の港湾設備および物流データプラットフォームが、海事分野のITシステムおよびOTシステムに脆弱性をもたらす可能性があると警告している。また、第三者からのネットワーク通信については、その安全性が検証されるまで信頼しないものとして扱うべきであるとしている。 港湾やターミナルのシステムとデータをやり取りする船舶、あるいは寄港中に陸上関係者へ船内ネットワークへのアクセスを許可する船舶は、それらの接続経路を通じてサイバーリスクにさらされる可能性がある。
詳細は、MARAD Maritime Security Communications with Industry (MSCI) Advisory 2026-014 を参照。

4.0 推奨される対応

4.1 この脅威への対策については、既存のガイダンスですでに示されており、本通知では重複を避けるため再掲しない。 会社は、RMI Marine Notice (MN) 2-011-13 に基づき、安全管理システムの中でサイバーリスクを管理するとともに、MN 2-011-16 に基づき、船舶保安計画の中でもサイバーリスクを管理する事。
その際の指針として、RMI Marine Guideline (MG) 2-11-16、IMO Circular MSC FAL.1/Circ.3/Rev.4、The Guidelines on Cyber Security Onboard Shipsを考慮する事。
また、関連する参考資料は Maritime Cyber Risk Management Resources (MARSEC-200) に掲載されている。[2]

4.2 上記で説明した事案を踏まえ、また4.1項に示された対策に基づき、会社は以下の事項が確実に実施されていることを再確認する事。

.1 ファイアウォール、ルーター、衛星通信端末、およびVPN装置の管理用インターフェースがインターネットから直接到達可能な状態になっていないこと。 また、遠隔管理が業務上必要な場合には、そのアクセスをあらかじめ指定された特定のIPアドレスのみに制限するとともに、多要素認証 (MFA) によって保護されていること。

.2 また、これらの機器のファームウェアが、現在もサポートされている最新版で稼働していることを確認し、サポート終了となった機器については、ネットワーク境界に残したまま使用を継続するのではなく、交換すること。 詳細については、米国サイバーセキュリティ・インフラセキュリティ庁 (CISA) の Binding Operational Directive 26-02 を参照のこと。[3]

.3 デフォルトアカウント、休眠アカウント、共有アカウント、および退職・異動等により不要となった利用者アカウントが削除されていることを確認するとともに、使用していないサービス、VPNポータル、およびリモート管理プロトコルが無効化されていることを確認すること。

.4 船内システムに対するリモートアクセス権を保有するすべての関係者が特定されていること、またそのアクセスが明確な目的と期間を定めた上で付与され、監督および記録の対象となっていること、さらに恒常的な無監督アクセスが撤廃されていることを確認すること。 詳細については、MSCI Advisory 2026-014 も参照のこと。

---

2 IMO Circular MSC-FAL.1/Circ.3/Rev.4 は、2026年5月28日に発行された。これは、第50回FAL委員会および第111回海上安全委員会の承認を経て発行されたものであり、2025年4月4日付の Rev.3 に代わる最新版である。

3 Binding Operational Directive (BOD) 26-02, Mitigating Risk From End-of-Support Edge Devicesは、2026年2月5日に発行された。また、米国サイバーセキュリティ・インフラセキュリティ庁、FBI、および英国国家サイバーセキュリティセンターが共同で公表したファクトシートReducing the Attack Surface for End-of-Support Edge Devicesも参照。

注）本和訳はご参照頂き易い様に用意されたものでマーシャルアイランド海事局発行の公式文書ではありません。本和訳とマーシャルアイランド海事局発行の公式英語版内容に齟齬が生じた場合は常に英語版を正とします。

.5 ネットワーク機器においてログ記録が有効化されており、そのログが船外のシステムへ転送されるか、または定期的にエクスポートされていることを確認すること。 これは、これらの機器のログ保存領域が限定的であり、新しいイベントが記録されるにつれて過去のログが上書きされてしまうためである。

.6 ITネットワークとOTネットワークが分離されていること、また乗組員の福利厚生用インターネットアクセスから、航海システム、貨物制御システム、バラスト制御システム、または機関システムへ到達できる経路が存在しないことを確認すること。

4.3 船内でFortiGateまたは SSL-VPN ゲートウェイが設置されている場合は、Maritime Cyber Alert 02-26、ならびに JCSA-20261006-01 に示された対策を適用すべきである。
また、FortiBleed によって漏えいした認証情報は、ファームウェアを更新した後も引き続き有効な場合があることに留意すべきである。したがって、パッチ適用やファームウェア更新だけでは、この脆弱性への対応は完了したことにならない。

4.4 船内の担当者は、以下のいずれかの事象を認識した場合、遅滞なく会社保安責任者へ報告しなければならない；衛星通信の原因不明の喪失または性能低下、ネットワーク機器の予期しない再起動、ネットワーク機器の予期しない設定変更、ネットワーク機器への管理者による不審なログイン、ECDIS、GNSS、AIS、またはレーダーにおいて、独立した位置確認手段と一致しない挙動、船舶または会社がサイバー侵害を受けている可能性を示唆する外部者からの連絡

5.0 サイバー侵害の疑いがある場合の対処

5.1 最近発生した事案の調査から得られた教訓を踏まえ、弊局は、サイバー侵害が疑われる場合に以下の対応を検討することを推奨する。
これらの対応策は、USCGおよびFBIの Maritime Cyber Alert 02-26、ならびにFBIおよび米国シークレットサービスの勧告 JCSA-20261006-01 に定められたインシデント対応措置を補完するものである。

.1 CSO、会社、および弊局へ遅滞なく通知するとともに、船舶が現在所在している、またはこれから入域しようとしている港湾国の当局にも通報すること。

.2 証拠は現状のまま保全すること。影響を受けたシステムまたはネットワーク機器については、影響範囲や侵害の実態が把握されるまで、再イメージ化 (OSの再インストール等)、初期化 (リセット)、再設定、ファームウェア更新、バックアップからの復元、または電源停止を行わないこと。

.3 特定された機器については、そのローカル保存領域のログが新たな記録によって上書きされる前に、ログおよび設定情報を直ちにエクスポートして保全するとともに、当該機器のアカウント一覧およびリモートアクセス設定についても保存すること。さらに、対象期間に係るVDRのデータを確保・保全すること。

.4 ワークステーションに対するアンチウイルススキャンは、ネットワーク機器内に保存されている情報を検査するものでもなければ、それらを保全するものでもないことを認識すること。 また、アンチウイルスによるスキャンは、ファイルの最終アクセス日時を変更する可能性があり、調査に必要な証拠を隔離または削除する可能性がある。スキャンを実施した場合には、隔離領域の内容、スキャンログを保全し、どのソフトウェアを実行し・いつ実行したか・その結果どうなったかを記録しておくこと。

注）本和訳はご参照頂き易い様に用意されたものでマーシャルアイランド海事局発行の公式文書ではありません。本和訳とマーシャルアイランド海事局発行の公式英語版内容に齟齬が生じた場合は常に英語版を正とします。

.5 最初の兆候を認識した時点から、実施したすべての対応措置について、その実施時刻とともに記録すること。

.6 また、航海システム、機関システム、または貨物関連システムに影響が及んでいる、あるいはその可能性がある場合には、できるだけ早い段階で、会社が加入しているP&Iクラブ,および認定機関 (Recognized Organization: RO) に連絡し関与してもらう事。

5.2 港湾国または外国当局が船内システムの調査・検査を実施しようとする場合、弊局へ、事前にその旨の通知をすること、また、船舶システムまたはデータへのアクセスを規律する文書が実行・署名される前に、その写しの提供を受けることを求める。
そのような文書には、事実関係に関する表明が含まれたり、船主に代わって一定のリスクや責任を受け入れる内容が含まれたりする場合がある。したがって、会社からの明示的な書面指示がない限り、船長が単独で当該文書に署名・締結してはならない。

6.0 港湾国に関する考慮事項

6.1 USCGの最終規則 “Cybersecurity in the Marine Transportation System”, 90 FR 6298は、2025年7月16日に発効し、33 CFR Part 101, Subpart F に規定されている。 この規則は、米国籍船・規制対象施設に適用されるものであり、弊船籍船舶には直接適用されない。
しかしながら、USCGは、外国籍船におけるサイバーリスク管理の不備を示す兆候について、PSC検査時の監視・確認を強化する方針であることを示しており、その確認は、ISM Code、ISPS Codeの遵守状況を通じて行われる。[4]

6.2 懸念の理由が文書で示されないまま、また解除条件が明示されないまま、Captain of the Port (COTP) Order が発出される場合がある。
そのような命令が発出された場合、会社は当該命令の根拠となった事実や理由、および命令を解除するために満たすべき条件について、書面により説明を求め、その命令書の写しを 弊局へ提出する事。

7.0 インシデント報告

7.1 会社は、弊船籍船に関わるすべての海事サイバーインシデントについて、MG 2-11-16に従い”Report of Maritime Cyber Incident (MI-109-5)”を提出して、弊局へ報告する事。 提出された情報は秘密情報として取り扱われ、報告された事案が特定の船舶または会社に結び付けられて公表されることはない。
また、MN 2-011-16に定められた保安インシデントの報告義務も引き続き適用される。

7.2 外部の当事者から、船舶が侵害を受けた旨の通知が当社に対してなされた場合、その通知自体、ならびに当該通知によって特定されるデバイス、アドレス、またはインジケーターについては、調査結果を待つことなく、受領次第、弊局　に提供しなければならない。

---

4 Cybersecurity in the Marine Transportation System最終規則は、Federal Register）90 FR 6298として2025年1月17日に公表され、案件番号USCG-2022-0802の下で制定されたものであり、2025年7月16日に発効した。現在は、33 CFR Part 101.600に法典化されている

注） 本和訳はご参照頂き易い様に用意されたものでマーシャルアイランド海事局発行の公式文書ではありません。本和訳とマーシャルアイランド海事局発行の公式英語版内容に齟齬が生じた場合は常に英語版を正とします。

7.3 報告及び通知は時間を問わず次の連絡先まで; marsec@register-iri.com, dutyofficer@register-iri.com, +1 571 441 1885。

7.4 米国水域内にある船舶、または米国水域へ向航中の船舶がサイバーインシデントを認識した場合は、次の機関にも追加で報告しなければならない。USCG ; maritimecyber@uscg.mil , Coast Guard Cyber Command (24時間当直) ; +1 202 372 2904, National Response Center (NRC) ; +1 800 424 8802
また、港湾国当局のみに報告しても、上記7.1項で定められた 弊局への報告義務を満たしたことにはならない。
さらに、その他の米国政府機関への報告窓口については、MSCI Advisory 2026-014 に記載されている。

8.0 参照文書

.1 MN 2-011-16, International Ship and Port Facility Security (ISPS) Code

.2 MN 2-011-13, International Safety Management (ISM) Code

.3 MG 2-11-16, Maritime Cyber Risk Management

.4 Maritime Cyber Risk Management Resources (MARSEC-200)

.5 Global Maritime Security Contacts (MARSEC-210)

.6 IMO Circular MSC-FAL.1/Circ.3/Rev.4, Guidelines on Maritime Cyber Risk Management

.7 Shipping industry associations, The Guidelines on Cyber Security Onboard Ships, version 5

.8 USCG, Cybersecurity in the Marine Transportation System, 90 FR 6298

.9 33 CFR, Part 101, Subpart F, Cybersecurity

.10 US Maritime Administration, Maritime Security Communications with Industry advisories

.11 CISA Binding Operational Directive 26-02, Mitigating Risk From End-of-Support Edge Devices

.12 USCG and FBI, Maritime Cyber Alert 02-26, Fortinet FortiGate Vulnerabilities

.13 FBI and United States Secret Service, JCSA-20261006-01, FortiBleed Operations Continue Targeting Exposed Systems Leading to Reports of Lockouts

.14 MARAD, MSCI Advisory 2026-014, Worldwide-Foreign Adversarial Technological, Physical, and Cyber Influence

注）本和訳はご参照頂き易い様に用意されたものでマーシャルアイランド海事局発行の公式文書ではありません。本和訳とマーシャルアイランド海事局発行の公式英語版内容に齟齬が生じた場合は常に英語版を正とします。