



JAPAN P&I NEWS

組合員各位

船舶におけるサイバーセキュリティ対策について

今般、一般財団法人日本海事協会（ClassNK）から、「船舶におけるサイバーセキュリティマネジメントシステム認証ガイドライン（第2版）」が発行されました。

本ガイドライン第2版は、国際的に広く用いられている ISO/IEC 27001 および ISO/IEC 27002 を参考に最新化するとともに、審査における評価基準や求められる客観的証拠が明確化されています。また、各評価基準において外部要求事項との対応関係も示されています。詳細およびガイドライン（PDF）のダウンロードにつきましては、[ClassNK のウェブサイト「CSMS 認証について」](#)をご参照ください。

各船において、サイバーセキュリティ対策を一時的な対応にとどめることなく、日々の安全管理において実効性を維持・向上させる仕組みを構築することが重要です。サイバー攻撃は、単なるデータ漏洩にとどまらず、操船・推進機能の喪失による「衝突・座礁」や「海洋汚染・貨物損害」といった、重大な事故に直結するリスクです。組合員におかれましては、すでに SMS（安全管理システム）に組み込まれている CSMS（サイバーセキュリティマネジメントシステム）を改めて見直す際、運航現場で実際に起こりがちな具体的なリスクを想定し、さらなる運用・教育への反映にお役立ていただくことをお勧めいたします。

- **リスクアセスメントの実施と監査結果に基づく継続的改善**

サイバーリスクに対応するため、IT（情報技術）および OT（制御・運用技術）システムを識別し、定期的なリスクアセスメントを実施することが推奨されます。さらに、外部検査や内部監査において指摘された事項については、IT 管理責任者からアドバイスやフィードバックを受け、対策の必要性を検討することが有効です。指摘事項を一時的な対応で終わらせず、マネジメントレビュー等を通じて体制の有効性を検証し、CSMS の継続的な改善のサイクルを回すことが重要です。

- **保守業者等への対応とネットワーク管理**

日常の運航において、保守業者から機器のサービスレポートを本船の PC やプリンターで印刷するよう頼まれることや、業者が監視カメラの LAN と通信用 LAN を誤って接続してしまうといったトラブルのリスクが存在します。不用意な機器の接続を防ぐため、安全にデータを受け渡しできる専用の機器（端末等）を本船に備えることや、こうした状況に対応する運用手順を確立し、乗組員への周知・指導することが推奨されます。

- **私用デバイス・USB の利用制限と IT リテラシーの向上**

データの保存や移動のために本船の共有 PC に個人の USB メモリを接続する、個人のスマートフォンから業務用 Wi-Fi にアクセスする、あるいは船員が許可なくプライベート用の Wi-Fi アクセスポイントを設置するといった行動は、マルウェア感染のリスクを高めます。こうした行為を明確に

制限するとともに、最新のサイバーリスクに対する乗組員の理解を深めるための継続的な教育・啓発が望まれます。

- **インシデント発生時の「遅滞ない報告」とデータの保護**

船がサイバー被害に遭うことを想定した備えも重要です。サイバーインシデントが発生、あるいは検知された際は、被害の拡大を防ぐため、遅滞なく IT 管理者や関係者へ報告し指示を仰ぐ体制の徹底が第一歩となります。また、ECDIS の航海計画 (Passage Plan) は適切にバックアップし、無断編集を防ぐためにロックするなどのデータ保護手順を確立しておくことが不可欠です。

- **乗組員への継続的な教育と受講記録の保持**

サイバーセキュリティ対策の実効性を高めるためには、マニュアル等の整備にとどまらず、現場で運用を担う乗組員の正しい理解と実践が不可欠です。乗組員の交替時には、本船のセキュリティルールの周知 (乗船時教育) を確実に行うとともに、定期的な教育・訓練を実施することが重要です。また、実施した教育の記録を適切に保存・管理しておくことで、ルールの定着状況を会社として客観的に確認・維持し、船陸一体となった事故防止体制を強化することができます。

当組合は、今後も事故防止に向けて、専門的知見を元に最新情報を提供してまいります。

以上