これ以上、サイバーセキュリティを見過ごすことはできません

こちらは、英文記事「Ship operators cannot afford to turn a blind eye to cyber security」（2019 年 7 月 10 日付）の和訳です。

米国コーストガード（USCG）が、ある船舶でのサイバーインシデントの調査を実施したところ、当該船舶のネットワークのセキュリティリスクが、インシデント発生前に船員らの間では十分に認識されていたことが判明しました。

また、USCG が最近発表した **Marine Safety Alert 06-19** の中で、商船におけるサイバーインシデントについて、以下の調査結果が示されています。

「2019 年 2 月、ニューヨーク港およびニュージャージー州に向けて外洋航海中のある深喫水船において、ネットワークに影響を与える重大なサイバーインシデントの発生が報告されています。コーストガードが率いる、各省庁のサイバー専門家から成るチームがこの問題に対応し、船舶のネットワークと重要な制御システムの分析を実施しました。同チームは、検出されたマルウェアは船舶のコンピュータシステムの機能を大幅に低下させたが、重要な制御システムに対する影響はないと結論付けま

した。しかし、この調査により、有効なサイバーセキュリティ対策を講じずに船舶が運航されており、重要な船舶制御システムが重大な脆弱性にさらされていることが明らかになりました」

この調査結果において最も憂慮すべき点は、船舶のネットワークで検出されたセキュリティリスクが、インシデント発生前に船員らの間では十分に認識されていたということです。ほとんどの船員が、船舶のコンピュータネットワークを（銀行口座の確認などの）個人的な目的で利用したいと思わないほど信用していなかったにもかかわらず、電子海図の更新、貨物データの管理や、陸上施設、パイロット、エージェント、ポートステート当局との通信などの業務目的では使用していたのです。

推奨事項

サイバーインシデントの調査結果に基づき、USCG はサイバーセキュリティ向上のために運航者に以下の基本的な対策を講じることを強く推奨しています。

- 重要なシステムや機器への不正アクセス防止のため、船舶のネットワークを「サブネットワーク」へと分割する。
- 各船員に固有のパスワードまたは ID カードで保護されたネットワークプロファイルを作成し、複数の船員による一般的なログイン認証情報の重複使用を回避する。
- ユーザの業務遂行のために必要最低限のネットワークアクセス権のみ許可するなど、各ユーザの権限を制限する。
- USB ドライブを介してのデータ転送の際に使用する USB メモリやその他のデバイスなど、外部メディアを使用する際の明確な手順を確立する。
- 基本的なウイルス対策ソフトウェアをインストールする。
- ソフトウェアのパッチ/アップデートの管理手順を確立する。オペレーティングシステムやアプリケーションに影響を与える脆弱性は絶えず変化しているため、サイバー犯罪者からコンピュータシステムを保護するためには、タイムリーなアップデートが最も重要なステップの一つです。

また、USCG は以下のように述べています。*「マウスのクリック操作でエンジンを制御できることや、電子海図システムとナビゲーションシステムへの依存度が高まっていることから、適切なサイバーセキュリティ対策でこれらのシステムを保護することは、船舶への物理的アクセスの制限や従来の機械の定期メンテナンスと同じくらい重要です」*

その他の推奨事項については、2018 年 12 月 12 日の Gard Insight「It is time to strengthen your onboard cyber security procedures (船舶のサイバーセキュリティに対応する手続きを強化すべき段階)」を参照してください。

Gard によるサイバーセキュリティに関する安全意識向上キャンペーン

IMO（国際海事機関）は、船主および運航者に、2021 年までにサイバーリスク対策を船舶の安全管理システムに組み込むことを推奨していますが、サイバー犯罪者は今既に活動しています。資産であるデータを保護するためには、機密性、完全性、可用性をバランス良く維持することが不可欠です。サイバーセキュリティは、船舶のシステムやプロセスの設計方法だけでなく、その使用方法（つまり、ヒューマンファクター）にも左右されます。

したがって、船員に適切なトレーニングを実施して、サイバーインシデントを発見・報告できるようにしておくことが必要です。サイバーセキュリティ関連の事例の分析に基づいて、DNVGL と Gard は共同で**ロスプリベンション意識向上ビデオ（英語）**と、海運業界のサイバーインシデント対処方法についての推奨事項を記載したプレゼンテーションを作成しました。なお、これらの資料は、業界全体での取り組みの変更やルールの変更を提案するものではなく、個人の行動や対応の変更を促すことを狙ったものです。