ClassNK サイバーセキュリティアプローチ

日本海事協会は，船舶のサイバーセキュリティに対する基本的な考え方について，国際機関や海事関連団体の動向も踏まえ，「ClassNK サイバーセキュリティアプローチ」をまとめました。

１．最重要事項は安全運航の確保

船舶におけるサイバーセキュリティ対策の重要な目的は安全運航の確保です。そのためには，船舶の運航を支える情報技術(Information Technology，IT)のみならず運用技術(Operation Technology，OT)における可用性の確保が優先すべき要素となります。

IT/OT 双方のサイバーリスク低減に向け，船舶及び船上機器類のセキュリティ・バイ・デザインな設計，就航中のマネジメントシステムの構築等，物理的，技術的，組織的アプローチをバランス良く組み合わせた対策を提案していきます。

２．サイバーセキュリティ対策の階層を設定

サイバーセキュリティ対策をいくつかの階層で整理の上，それぞれの階層ごとに，既存のサイバーセキュリティに関する国際規格等から船舶に適用可能と考えられる要件を採用し，「どの関係者が何をすべきか」について，明確に示していきます。

３．継続的な見直しと最新化

船舶運航における IT 化の進展やサイバーセキュリティの国際動向を踏まえ，最新の情報を専門家と共に分析し，船舶におけるサイバーセキュリティ対策について，その時点におけるベストプラクティスを提案していきます。

これらの考え方に基づき，サイバーセキュリティ対策の実施主体者と対策内容を示したガイドラインや規格を「ClassNK サイバーセキュリティシリーズ」として，随時公表していきます。

ClassNK サイバーセキュリティアプローチ

船舶のサイバーセキュリティ対策の階層

1. ソフトウェア・ハードウェア装置による対策
2. 「装置対策」の健全性を保つための運用対策
3. 「運用対策」の健全性を保つための運用対策
4. 情報セキュリティマネジメントとして設計する組織的な対策
5. サイバーリスクを低減した船用製品の開発

1 2 3 船舶における サイバーセキュリティデザインガイドライン

対 象　造船所及び建造船主

- NIST SP800-82を参考に、NIST 800-53の中で船舶に適用できるものを抽出
- IACS Rec. の内容を精査

4 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

対 象　船舶管理会社及び船舶

- ISO27001及び27002の基本構造を参考にし、ISMコード体系との親和を図ったマネジメントシステム

5 ソフトウェアセキュリティガイドライン

対 象　船用機器メーカー

- ISO/IECの関係規格をベースに船用に必要な要素を抽出したガイドラインに基づき、その開発プロセスと機能要件を検証する