サイバーセキュリティに関するIMO/IACSの最新動向

一般財団法人日本海事協会
事業開発本部
認証企画室　室長　斎藤直樹

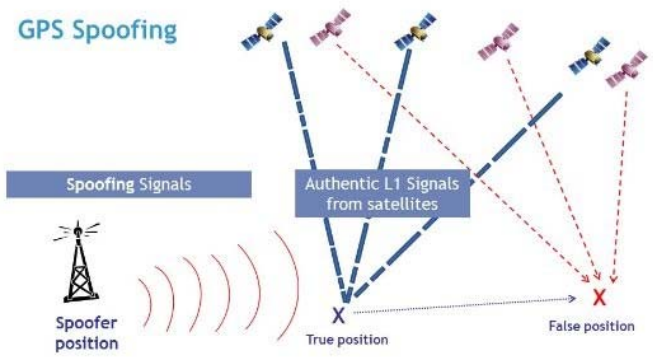
目　次

1. サイバーセキュリティ対策の背景
2. サイバーセキュリティに対する考え方
3. ガイドラインの公表
4. まとめ

サイバーセキュリティ対策の背景

2017年6月に黒海でGPS通信の操作で、航海中の船20隻のナビゲーション・システムが正常に作動していたにも関わらず、別の位置に誘導されていた事件があった。「スプーフィング」と呼ばれる技術が使われた疑いが高い。

2017年8月10日　NewScientist　より



- 「イランの脅威に米が警鐘、商船へGPS妨害や偽装通信ホルムズ海峡」（CNN:2019年8月8日）
- “GPS spoofing attack shows shipping is ‘driving with eyes closed”(Maritime Executives: 2019年8月29日)

サイバーセキュリティ対策の背景

USCG（米国沿岸警備隊）:
商船に対するサイバー攻撃に関する海事安全情報を発出

2019年5月24日

- port@pscgov.org というあたかもPSC当局のようなメールアドレスを使用
- 到着通知(Notice of Arrival)に含まれる機密情報を抜き取ろうとする
- 船上のコンピューターシステムに害を与える悪意のあるソフトウェアについてもUSCGは報告を受けている
- USCGは船舶運航者等へ，自船におけるサイバー攻撃に対する防御策を継続的に評価するように求めている。

サイバーセキュリティ対策の背景

ClassNK Consulting Service

USCG（米国沿岸警備隊）：
サイバーインシデントに対する商船の潜在的な脆弱性

2019年7月8日

- 2019年2月にニューヨーク港向け大型商船の船上ネットワークに重大なサイバーインシデントが発覚
- USCGの調査チームによれば、船上のコンピューターシステムがマルウェアの影響を受けたが、運航に関する制御システムには影響がなかった。
- USCGは船舶運航者等へネットワーク、パスワード、取り外し可能媒体（USB）、アンチウィルスソフト、パッチにおけるサイバーセキュリティとしての基本的な対策を強く推奨している。

サイバーセキュリティ対策の背景

ClassNK Consulting Service

港湾施設等へのサイバー攻撃

- 2013年　アントワープ港（税関システムを乗っ取り、コカインの密輸に成功）
- 2017年　船会社クラークソン（UK）（情報を盗み取られるもランサムウェア脅迫を拒否）
- 2017年　マースク（対応コストは約330億円。システム復旧まで手作業で対応）
- 2018年　コスコ（米国法人）
- 2018年　バルセロナ港
- 2018年　サンディエゴ港

サイバーセキュリティ対策の背景

2021年からISMコードでサイバーリスクを扱うことが事実上要求される見込みです

IMO（国際海事機関）第98回海上安全委員会 (2017年6月)

MSC決議

"安全管理システムにおける海事サイバーリスクマネジメント"

(Res. MSC.428(98))

要旨:

1. ISMコードの目的及び機能要件に従って、サイバーリスクマネジメントを安全管理システムにおいて考慮されるべき
2. **2021年1月1日より後**、最初のDOC年次審査までに、サイバーリスクが安全管理システムで適切に対処されてること（RO等による確認）

上記決議に関するサーキュラーをすでに発出した主な旗国:

マーシャル諸島、リベリア、香港、パナマ、ドイツ、USCG（米国）等

サイバーセキュリティ対策の背景

国際船級協会連合（IACS）はサイバーセキュリティに関する推奨事項を公表しました

■ **サイバーシステムパネル (2016年7月～)**

12のRecommendationsを策定（2018年11月に公表）

No.153 ソフトウェア保守手順	159 ネットワークセキュリティ
154 機器の手動/機側制御	160 船舶システムデザイン
155 緊急時対応計画	161 インベントリリスト
156 ネットワーク構造	162 インテグレーション
157 データの保証	163 遠隔アップデート/アクセス
158 物理的セキュリティ	164 通信及びインターフェース

現在、12のRecommendationsを1つに統合する作業を実施中

サイバーセキュリティ対策の背景

オイルメジャーの検船スキーム等ではすでにサイバーセキュリティに関する推奨事項が検査対象とされています

OCIMF（石油会社国際海事評議会）

推奨事項：

1. サイバーセキュリティに関する内部監査プログラムを実施すること
2. 船舶所有者が独立したサイバーセキュリティ専門家のサポートを得ること
3. サイバーセキュリティリスクに対処するため、ISMシステム／SMS及びISPS Ship Security Planを更新すること

Right Ship Dry Bulk Inspections

ISMコード　推奨事項：

1. サイバーセキュリティの手順の確立と要員に対する訓練の実施
2. 上記手順にはリスクアセスメントとサイバー攻撃時の緊急計画を含む

サイバーセキュリティ対策の背景

サイバー攻撃の最新情報の収集

国際的な情報収集活動

1. Maritime Cyber Security Emergency Response Team (MCERT)

- 運営主体：Templar Executives社（UK）とWartsilaが共同運営
- 拠点：シンガポール

https://www.templarexecs.com/mcert/

2. Maritime Cyber Alliance

- 運営主体：CSO Alliance (UK)
- 拠点：ロンドン

https://www.maritimecyberalliance.com/

サイバーセキュリティの教育

Templar Executives社（UK）

“Cyber Security Awareness e-Learning for the Maritime Industry”の認証

（2019年5月）

- BIMCOガイドラインの“Training and Awareness”を網羅
- 英国の政府通信本部（GCHQ)の認証も取得

https://www.templarexecs.com/gchq-classnk-certified-cyber-security-awareness-e-learning-for-maritime/

船舶保険業界におけるサイバーリスク対応

1. 現在、世界各国の船舶保険マーケットにおいて適用されている約款では、**サイバー攻撃による損害は免責から除外**されている。
2. サイバーリスクの高まりを受け、近年のロンドンマーケットではこの約款に加えて、“Institute Cyber Attack Exclusion Clause（01/11/2003）(Cl.380)” を付帯するケースが増えている。
3. “Institute Cyber Attack Exclusion Clause（01/11/2003） (Cl.380)”では、**サイバー攻撃による損害を全面的に免責**とするもので、**海運業界のデジタライゼーションに伴って普及しつつあると言える。**

出典：2017年11月「海運」 海上保険特集 「海運業界におけるサイバーリスクと保険」（東京海上日動）

船舶保険業界におけるサイバーリスク対応

Cl.380のBuy-Back保険の登場

1. SIGCo（バミューダ諸島：主に米国向け）のCyber Hull Insurance
https://www.sigcogroup.com/services-products/cyber-hull-insurance.php

2. Norwegian Hull Club（ノルウェー）のCl.380 buy-back cover
https://www.norclub.com/products/special-risks/cyber-clause-380-buy-back-/

3. Beazley（UK）のCyber defence for marine
https://www.beazley.com/london_market/marine/marine_cyber.html

4. Lampe & Schwartze（ドイツ）のShip Owners' Marine Cyber Cover
https://www.lampe-schwartze-marine.de/home

1. サイバーセキュリティ対策の背景
2. サイバーセキュリティに対する考え方
3. ガイドラインの公表
4. まとめ

サイバーセキュリティに対する考え方

ClassNK Consulting Service

日本海事協会としての基本的な考え方を「ClassNK サイバーセキュリティアプローチ」として公表しました（2019年2月）

1. 最重要事項は安全運航の確保

- 船舶の運航を支えるIT及びOTにおける可用性の確保を優先
- 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

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
- 階層ごとに、既存の情報セキュリティの国際規格等から船舶へ適用可能な部分を採用し、「どの関係者が何をすべきか」について明確化

3. 継続的な見直しと最新化

- 最新のサイバーセキュリティ情報を専門家と共に分析
- 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

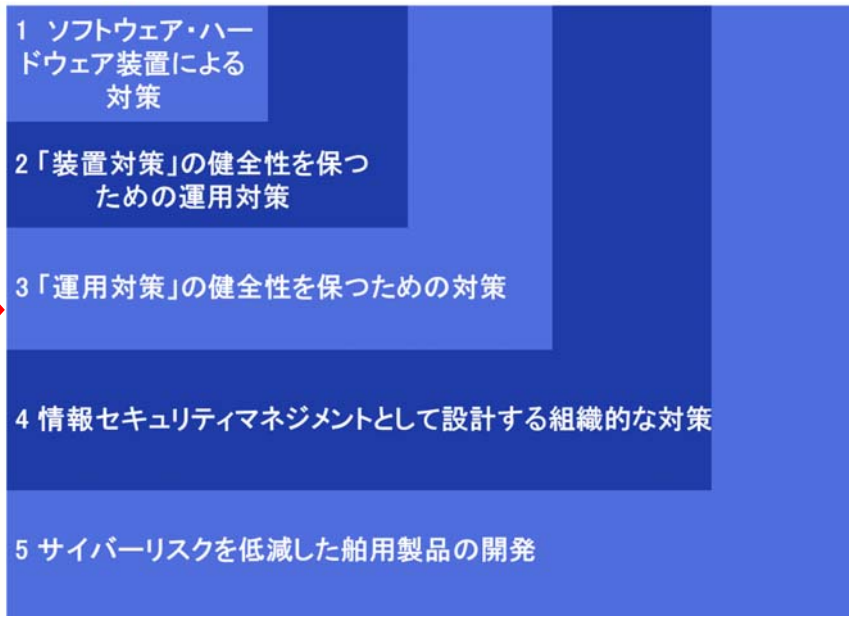
サイバーセキュリティに対する考え方

ClassNK Consulting Service

船舶のサイバーセキュリティ対策の階層を設定しました

ClassNKサイバーセキュリティアプローチ

1. 最重要事項は安全運航の確保
2. サイバーセキュリティ対策の階層を設定
3. 継続的な見直しと最新化



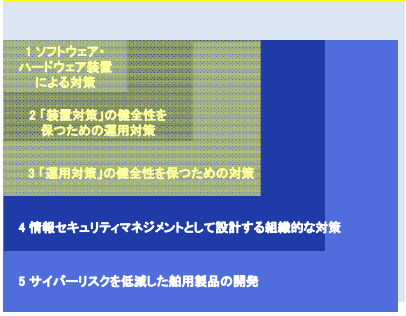
1. サイバーセキュリティ対策の背景
2. サイバーセキュリティに対する考え方
3. ガイドラインの公表
4. まとめ

ガイドラインの公表

「ClassNK サイバーセキュリティアプローチ」に基づくガイドラインの公表を開始しました

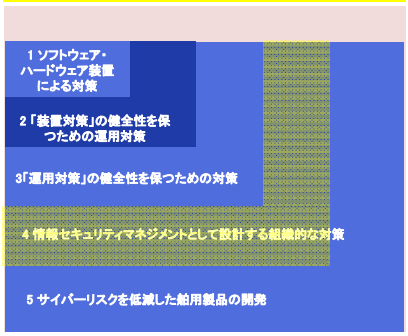
（本会ウェブサイトにてマイページのユーザー登録をすることにより、ご覧いただけます）

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



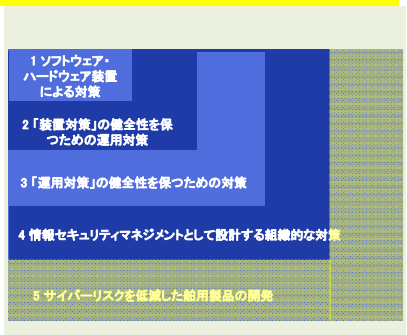
2019年2月公表

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



2019年2月公表

ソフトウェアセキュリティ ガイドライン



2019年6月公表

ガイドラインの公表

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

2019年2月　第1版

- 対象：造船所及び建造船主
- NIST SP800-82を参考に，NIST SP800-53の中で船舶に適用できるものを抽出
- IACS Rec.の内容を精査

ガイドラインの公表

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

（要求事項及び管理策）
2019年2月　第1版

- 対象：**船舶管理会社**及び**船舶**に**証書**を発給
- 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

認証サービスを早期に開始予定

認証取得のポイント

- リスクアセスメントの実施
- リスクアセスメントに基づく管理策の実施

ガイドラインの公表

ClassNK Consulting Service

ISMコードとは別にサイバーセキュリティマネジメントシステム（CSMS）を構築するスキームが主流になると見られています

2021年1月1日から安全管理システムの中で、サイバーリスクを取り扱うことが事実上強制化

ISMコードの目的：海上における安全、人命及び海洋環境の保護

サイバーセキュリティの目的：資産と情報の保護

安全管理システムの中へサイバーリスク管理を取り込む基本的な考え方：

「資産や情報の可用性や完全性が損なわれた結果として、人命の損失及び船舶・海洋環境が損害するリスク管理を継続的に実施すること。またサイバーリスク管理が有効に機能するために資産や情報を適切に保護する対策を講じること」

オイルメジャーやRightShipの検船ではISMコードの目的や機能要件以上のサイバーセキュリティ対策が必要となることが予想される

「ISMコード」と「サイバーセキュリティ」という**直接的な目的が異なるものを統合することが現段階では難しい**ことやオイルメジャー、RightShip検船対策、船舶保険向けとして、**ISMコード対応とは別にCSMSを会社と船で構築する**スキームが主流になると見られており、他船級はCSMS認証サービスを開始

ガイドラインの公表

ClassNK Consulting Service

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

	ISMコード	サイバーセキュリティマネジメントシステム	ISMS関連の相当規格
管理システム	安全管理システムの要件 ISMコード　A部：実施 1 一般 2 安全及び環境保護の方針 3 会社の責任及び権限 4 管理責任者 5 船長の責任及び権限 6 経営資源及び要員配置 7 船内業務 8 緊急事態への対処 9 不適合、事故及び危険発生の報告及び解析 10 船舶及び設備の保守 11 文書管理 12 会社による検証、見直し及び評価	サイバーセキュリティ管理システムの要件 第1部　要求事項 1 一般 2 サイバーセキュリティ方針 3 会社の責任及び権限 4 管理責任者 5 船長の責任及び権限 6 経営資源及び要員配置 7 船内業務 8 緊急事態への準備 9 不適合、事故及び危険発生の報告及び調査・解析 10 船舶及び設備の保守 11 文書管理 12 会社による検証、見直し及び評価	ISO/IEC 27001 本文
認証	ISMコード　B部：証書発給及び検証	サイバーセキュリティ マネジメントシステム認証基準	
対策（管理策）		第2部　サイバーセキュリティ対策 1 一般 2 造船における管理策 3 運航における会社の管理策 4 運航における船舶の管理策	ISO/IEC 27001 Annex A ISO/IEC 27002

ガイドラインの公表

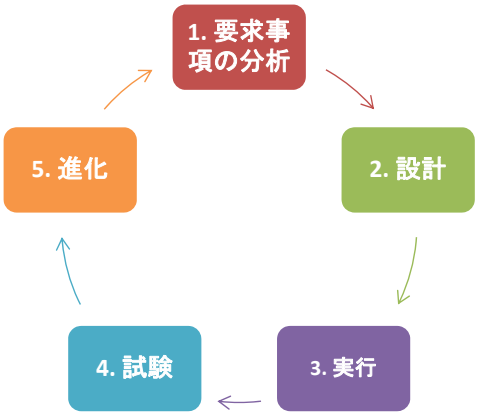
ClassNK Consulting Service

ソフトウェアセキュリティガイドライン

認証サービスをすでに開始

2019年5月　第1版

- 対象：舶用機器メーカー
- ISO/IECの関係規格をベースに舶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



ガイドラインの公表

ClassNK Consulting Service

テュフラインランド とのパートナーシップを締結しました

ClassNK　TÜVRheinland

2018年10月30日にサイバーセキュリティに関する認証事業におけるパートナーシップを締結

具体的な連携：

1. ソフトウェアセキュリティガイドラインの策定
2. サイバーセキュリティマネジメントシステムの認証基準の策定

左：テュフラインランド：ミヒャエル フビCEO
右：日本海事協会：冨士原康一会長
(2018年10月30日、東京)

今後のガイドライン検討の方向性

1. セキュリティ・バイ・デザインな船舶へ向けた取組み
2. IACS 統一規則 E22（コンピューターシステム）におけるシステム分類を基本に既存のセキュリティ規格を船舶に応用
3. OT（運用・制御技術）とIT（情報技術）の視点から、供給者、統合者、所有者が満たすべきセキュリティ要件を具体化
4. 具体的にOT的視点としては制御システムセキュリティ基準としてのIEC62443とIT的視点としてはISO27001（情報セキュリティマネジメントシステム）の要件が基本
5. IACS統合Recommendationを注視

IACS 統一規則 E22（コンピューターシステム）におけるシステム分類

分類	故障時の影響度合い	システムの機能
Ⅰ	故障が人体及び船体への危険並びに環境への脅威に帰結するおそれのないシステム	- 情報収集又は管理業務に関するシステム
Ⅱ	故障が人体及び船体への危険並びに環境への脅威にゆくゆくは帰結するおそれのあるシステム	- 警報及び監視機能 - 船舶の正常な操船及び居住状態を維持するための制御システム
Ⅲ	故障が人体及び船体への危険並びに環境への脅威に直ちに帰結するおそれのあるシステム	- 推進及び操舵に関連する制御システム - 安全システム

- **通常分類Ⅲの例**：(1) 船舶の推進システム (2) 操舵制御システム (3) 電源システム (4) 安全システム（火災探知及び消火，浸水検知及び対応，非常用を含む船内通信システム及び救命設備の運用に供するもの） (5) 自動船位保持装置 (6) 掘削装置
- **通常分類Ⅱの例**：(1) 液体貨物移送制御システム (2) ビルジ高液面検知装置及び関連するポンプの制御装置 (3) 燃料油操作システム (4) バラスト移送用弁の制御システム (5) 船舶の安定及び浮揚制御システム (6) 推進システムの警報及び監視システム

1. サイバーセキュリティ対策の背景
2. サイバーセキュリティに対する考え方
3. ガイドラインの公表
4. まとめ

まとめ

- 2021年以降はISMコードにおいて、サイバーリスクを扱うことが事実上要求される
- 上記の対応として、ISMコードとは別にサイバーセキュリティマネジメントシステム（CSMS）を構築するスキームが主流になる見込み
- IACSが公表した12の推奨事項の統合とその後の展開を踏まえた船舶設計レベルでのサイバーセキュリティ対策の動向を注視
- サイバーリスクに関する船舶保険の動向を注視

2019年9月
サイバーセキュリティプロジェクトチームを設置

- 本会関係各部の船舶及びセキュリティに関わる専門家を結集した部門横断組織
- 専門機関との連携をさらに強化及び拡大

目標:
発行したガイドラインに基づく認証の早期提供開始

サイバーセキュリティに関するお問い合わせ:
日本海事協会　事業開発本部　認証企画室
電話:03-5227-2177
e-mail: met@classnk.or.jp

サイバーセキュリティに関するIMO/IACSの最新動向

1. はじめに

非強制ガイドライン MSC 決議“安全管理システムにおける海事サイバーリスクマネジメント”(Res. MSC.428(98))に基づき、2021年からISMコードでサイバーリスクを扱うことが事実上要求される見込みである。IACS(国際船級協会)をはじめとする関係団体が、具体的な船舶のサイバーセキュリティ対策の議論が進められている中で、弊会は今年に入り、船舶のサイバーセキュリティに関する基本的な考え方をまとめ、3つのガイドラインを公表している。

そこで本講演では、現在の海上におけるサイバー攻撃の現状や IMO/IACS の最新動向を紹介し、弊会としてのサイバーセキュリティサービスを紹介する。

2. サイバーセキュリティに関するIMO/IACSの最新動向

① サイバーセキュリティ対策の背景
最近の海上サイバー攻撃事例を紹介し、IMO 及び IACS の動向、業界団体の動向を紹介する。

② サイバーセキュリティに対する考え方
日本海事協会としての基本的な考え方を示した「ClassNK サイバーセキュリティアプローチ」を説明する。

③ ガイドラインの公表
これまでに公表したガイドラインを説明するとともに今後のサイバーセキュリティサービス展開について紹介する。

3. おわりに

船舶のサイバーセキュリティについては、関連する国際規格をどのように船舶に適用できるのかを引き続き精査する一方で、GPSスプーフィングといった船舶における新たな脅威や陸上のサイバー攻撃手法についての情報収集及び分析を進め、専門機関との連携を強化し、NKとして最新のサイバーセキュリティサービスを提供していけるように努めて参る所存である。