

# CYBER RISK MANAGEMENT

---

2020年12月

海工務部

**船舶管理会社 (DOC Holder) に対して、2021年1月1日より後の最初の DOC年次審査までに、サイバーリスク管理が ISMコードに則り SMS で適切に対処されていることをIMOが推奨するガイドラインが採択された**

- 旗国によっては IMOガイドラインを強制としている
- 米国は IMOガイドラインを基に独自の規則を発行しており、寄港するすべての船舶が対象

※ タンカーはサイバーリスク管理についてSIRE検査の項目があり、既に管理会社はSMSで対処しているので、主にバルカーのみを取り扱う船舶管理会社の対処が必要と考える

## 各旗国・寄港国のIMOガイドラインに対する措置

**強制とする旗国** : Marshall Islands, Cayman, Cyprus, Australia, Bahamas, UK, Liberia, Singapore, Vanuatu, Norway, Myanmar, Palau, USA, Bermuda, Germany, Denmark

**推奨とする旗国** : Panama, Hong Kong, Japan

**強制とする寄港国** : USA

IMOとは別に独自の規則 : Vessel Cyber Risk Management Work Instruction (CVC-WI-027(I))

不備がある場合は Action code 17 (出港前是正) もしくは Action code 30 (拘留) となる

※ 2020年12月1日調べ

## 求められるサイバーリスク管理

IMO発行ガイドラインに記載の要求事項をSMSに取り入れる必要がある

- IMO Resolution MSC.428(98)
- MSC-FAL.1/Circ.3

### IMO Resolution MSC.428(98)において推奨される別機関発行のガイドライン

- The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
- ISO/IEC 27001 standard on Information technology – Security techniques –Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework)

### 各船級 設計・建造系ガイドライン・認証サービス

- ClassNK : 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)(第1版) / 船舶におけるサイバーセキュリティーデザインガイドライン(第2版)
- ABS : CYBERSAFETY CS / CS Ready
- LR : ShipRight
- BV : SYS-COM, CYBER SECURE
- DNV-GL : Cyber secure (Advanced)



# 何をSMSに取入れたらいいのか？

IMO Resolution MSC.428(98)において”Safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code”との記載があることから、Cyber Risk ManagementのSMSへの取入れにおいて推奨される項目は以下が考えられる

ISMコードにおける要求事項	該当ISMコード	
自社のスタンダードを制定する	ISM code 2	Company's Cyber Security Policy
IT管理者を選任する	ISM Code 3.2	Responsible Person of Cyber Risk Management
リスクアセスメント・必要な対策の制定	ISM Code 1.2 & 1.4	Assessment of Cyber Risks and Establishment of its Safeguards
ITシステムの洗い出し(リスト化)	ISM Code 6	Resources and Personnel
実施・運用	ISM Code 10	Shipboard Operation
見直し・改善・インシデント統計分析	ISM Code 12	Company Verification, Review and Evaluation
旗国特別要件 (現在は特に無し)	ISM Code 1.2.3.2	Special requirements of Flag States

どの程度の対策をすれば良いか、管理会社で行ったサイバーリスクアセスメントの結果と会社方針によって異なる

ITについてわからない、マニュアル作成についてどうしたら良いのか?、他の仕事で忙しいなどといった場合は支援サービスを提供するコンサルタント会社を起用することも一案

- ・ 株式会社オルカ
- ・ 株式会社ClassNKコンサルティングサービス  
など
- ・ 海力株式会社
- ・ 株式会社 KPMG FAS

### **DOC : Document Of Compliance / 適合証書**

SOLAS条約付属書第IX章4規則1に規定され、ISMコードの要件への適合に関する最初の検査に合格した場合、旗国の権限の下に船舶管理会社に発行される証書。毎年 年次審査を受けることを条件に証書有効期限は5年間。

### **ISMコード : International Safety Management Code / 国際安全管理コード**

海難事故防止のため人的要因の重要性が国際的に認識され、船舶の安全管理の強化が求められたことにより「国際安全管理コード (ISM Code)」が SOLAS条約 IX章に取り入れられた。これにより、2002年7月1日以降、国際航海に従事する高速旅客船を含む客船、500総トン以上の全ての貨物船及び移動式海底資源掘削ユニットとそれらの運行管理を行う会社に対し「ISMコード」が強制適用される。

### **SMS : Safety Management System / 安全管理システム**

船舶管理会社はISMコードに則った安全管理システム(SMS)を構築し、文書化し、実施、維持した上で、旗国政府の審査を受け、適合証書を取得し、船舶には安全管理証書(SMC)を備え置かなければ、外航運輸事業に従事出来ないことになっている。