



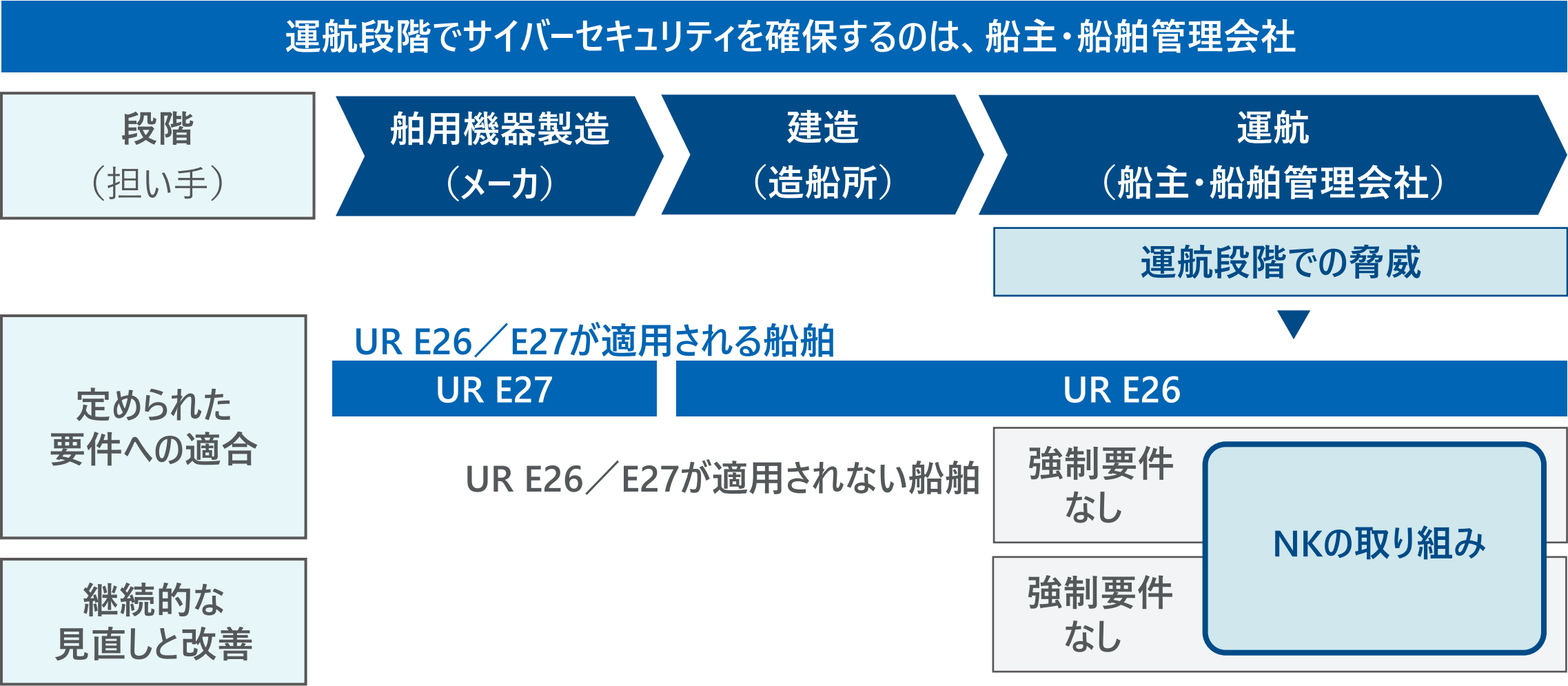
ClassNKサイバーセキュリティ マネジメントシステム ガイドライン改訂版の紹介

一般財団法人日本海事協会 船舶管理システム部

本日の内容

1. 就航している船を取り巻く状況と本会の取り組み
2. ガイドライン改訂版のご紹介
 - 2.1 先進的な安全対策に関するガイドライン（a-SAFE）
 - 2.2 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（CybR-G）
 - 2.3 ClassNKサイバーセキュリティマネジメントシステムガイドライン（CSMS）
3. おわりに

船舶のライフサイクルとセキュリティ対策



さまざまな脅威があるなかで、拠るべき基準が十分でない就航している船への取り組み

就航している船を取り巻く3つの脅威

いずれも、これまで拠るべき基準が十分でなかった

脅威	求められるもの
GNSS（全球測位衛星システム）への電波妨害 ・2026年3月、ペルシャ湾地域で650隻超に影響 ・自船の位置が把握できず、ビジネスの継続性にも影響	妨害に気づく備え
船内システムのサイバーリスク ・船内情報系（IT）と運航機器系（OT）のネットワークが未分離 ・保守業者のリモート接続、USBデバイスの持ち込み	船の対策を示すもの
外部要求の増加 ・傭船者等からセキュリティ管理体制について問われる機会が増加 ・類似した要求が、それぞれ独自の様式で示される	会社として対応する仕組み

NKの3つの取り組み

求められるものに、それぞれ応えるガイドラインを改訂した

求められるもの	改訂したガイドライン	確認する内容
妨害に気づく備え	先進的な安全対策に関するガイドライン	GNSSへの電波妨害を検知し、警報を発する設備
船の対策を示すもの	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	船内システムへの技術的な対策
会社として対応する仕組み	ClassNKサイバーセキュリティマネジメントシステムガイドライン	マネジメントシステムの構築・運用

取得できるNotationと認証

取り組みを船級符号や認証として示せる

名称	種別	お示しいただけること
a-SAFE(GIMS)	Notation	安全な運航の継続を支える機能があること
CybR-G(ES)	Notation	就航している船として必要な対策が講じられていること
マネジメント システム認証	認証	会社と船舶が一体でサイバーリスクを継続的に管理していること

いずれも取得は任意

2.1

先進的な安全対策に関する ガイドライン

a-SAFE

a-SAFE ガイドライン | ガイドラインの概要と改訂の背景

先進的な取組みを評価する枠組みに、GNSSへの電波妨害への対策を加えた

先進的な安全対策に関するガイドライン（2022年4月 第1版）

鋼船規則が船舶の安全性を評価するのに対し、先進的な取組みを第三者として評価する枠組み
これまでに5つの付記を設けている（波浪や浮氷の表示、衝突リスクの予測・警告等）

改訂の背景

妨害の発生

GNSSへの電波妨害が現に発生し、船舶の運航に影響が及んでいる

機器側の対応

妨害対策アンテナ、妨害電波検知機能を有する機器などが登場

枠組みの不在

5つの付記は、いずれもGNSSへの電波妨害を対象としていない

a-SAFE ガイドライン | a-SAFE(GIMS)の新設

GNSSへの電波妨害を検知し、警報を発する機能を備えた船舶への付記を新設した

ガイドライン 3.2.6

要件 ジャミング（電波妨害）及びスプーフィング（なりすまし）による影響を検知し、その旨の警報を発することによって船員の状況認識を支援するシステムを備えること

付記 *Advanced Safety (GNSS Interference Mitigation System)* 略号 *a-SAFE(GIMS)*

「警報を発すること」を要件とした理由

妨害そのものを船側で防ぐことはできない



まず気づくことが、安全な運航を継続するための出発点となる



検知した情報が乗組員に伝わることで、状況に応じた判断ができる

a-SAFE ガイドライン | 対象となり得るシステム

妨害への対策には、複数の方法がある

例えば、次のようなシステムが該当する

妨害対策アンテナ

妨害電波の影響を受けにくい構造

妨害電波検知機能を有する機器

妨害を検知する機能を備えた機器

マルチコンステレーション受信機

複数の衛星測位システムを利用

マルチ周波数受信機

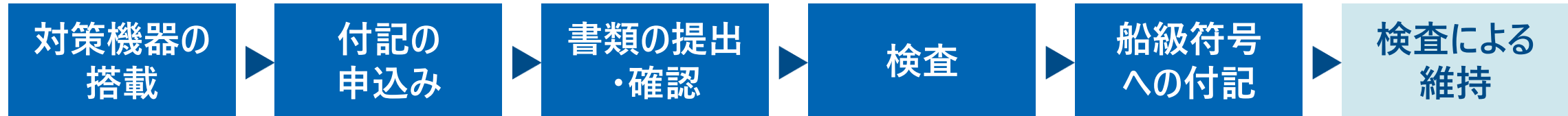
複数の周波数帯を利用

警報の構成

機器自体が発報する構成のほか、船内の警報装置と接続して報知する構成も対象となる

a-SAFE ガイドライン | 付記までの流れ

機器の搭載後に、申込みから取得できる



提出書類

- (1) システム概要
- (2) オペレーションマニュアル
- (3) 電気配線系統図
- (4) 社内試験成績書

確認する事項

- (1) 警報の発報条件
- (2) 報知方法

a-SAFE ガイドライン | まとめ

GNSSへの電波妨害に備えていることを、船級符号で示せる

新設した付記

a-SAFE(GIMS)

GNSSへの電波妨害に備えた船舶の船級符号に付記する。

要件

妨害の検知と警報

妨害の影響を検知し、その旨の警報を発することが要件。

2.2

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

CybR-G

CybR-G ガイドライン | ガイドラインの概要と改訂の背景

就航している船を対象としたサイバーセキュリティ対策の推奨事項が検討された

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 第1版）

設計段階からサイバーセキュリティを考慮することを示したガイドライン（新造船向け）
対策を講じた船舶の船級符号に付記する枠組みを設けている

改訂の背景

新造船

UR E26／E27により、サイバーセキュリティが義務化された

就航している船舶

新造船と同様に、サイバーセキュリティ対策が求められてきた

IACS

1年をかけて、就航している船舶に向けた推奨事項を検討

CybR-G ガイドライン | CybR-G(ES)の新設

就航している船舶が実施できる管理策を講じた場合に、新たな付記を設けた

新設する付記

Cyber Resilience-Guideline for Existing Ships 略号 *CybR-G(ES)*

サイバーセキュリティ対策を講じた船舶の船級符号に付記する

IACS Recommendation No.194

Cybersecurity Controls for Existing Ships (2025年12月)

IACS (国際船級協会連合) が、就航している船舶に向けて示した推奨事項

UR E26が新造船に求めるサイバーセキュリティ対策のうち、就航している船でも実施できるものを14項目の管理策として整理したもの

CybR-G ガイドライン | Rec.194が示す管理策

識別から復旧まで、5つの機能にわたる管理策が示されている

識別	防御		検知	復旧
1. 資産の把握	2. ネットワーク防御	6. 遠隔アクセス	10. ネットワーク監視	13. バックアップ
	3. ウイルス対策	7. 可搬デバイス	対応	14. 復旧対応
	4. アクセス制御	8. 教育	11. 陸上の連絡窓口	
	5. 無線通信	9. 更新・保守	12. 報告	

CybR-G ガイドライン | 付記までの流れ

管理策の実施後に、申込みから取得できる



対象となる船舶

2024年7月1日より前に建造契約が行われた船舶

対象とするシステム

船舶の運航を監視・制御するシステム（OTシステム）
推進、操舵、電源、航海、火災探知 など
これらが他のシステムとつながるシステム・ネットワーク機器

CybR-G ガイドライン | まとめ

就航している船舶として必要な対策を講じていることを、船級符号で示せる

新設する付記

CybR-G(ES)

サイバーセキュリティ対策を講じた船舶に付記する。
UR E26から、就航している船舶でも実施できるものを整理した対策。

対象

就航している船舶

2024年7月1日より前に建造契約が行われた船舶。
運航を監視・制御するシステムと、これらと直接つながる機器が対象となる。

2.3

ClassNKサイバーセキュリティマネジメントシステム ガイドライン CSMS

サイバーセキュリティマネジメントシステム（CSMS）ガイドラインとは

CSMS = サイバーリスク対応を日々の業務の中に組み込み、継続的に運用・改善する仕組み

デジタル化

サイバーリスクの発生

陸上へのデータ転送

海図の自動更新

等

船舶のデジタル化に伴いサイバーリスクが生じ、個別の脅威への都度対応ではなく、会社のマネジメントの中で管理することが必要になった。

2017年

IMO 決議 MSC.428(98)

サイバーリスクを、ISMコードのもとで会社が管理すべきものとして明確に位置づけた。

2019年

CSMS ガイドライン発行

会社の管理体制が適切に構築・運用されているかを、第三者として検証するサービスを提供。

CSMS ガイドライン | ガイドラインの構成

現行版の構成を見直し、要求事項・審査基準・外部要求との対応が一体で分かる形に組み直した

現行版（2019年）の構成

第 1 部 要求事項	第 2 部 管理策
ISMコードの体系との親和を図った、会社及び船舶に適用するCSMSの要求事項	造船・運航において実施する管理策と実施の手引



改訂版（2026年）の構成

第1部	第2部 NK CSMS 要求事項		業界要求との対応					
条文	評価基準	客観的証拠	RISQ	DryBMS	SIRE	TMSA	FAL	Rec.194

CSMS ガイドライン | 改訂（1）国際標準との整合

ISMコードの構造を維持しつつ、ISO 27001・27002 の体系を踏まえて条文を最新化した

- ・審査の場で個別に参照していた国際標準を、**要求事項**として位置付けた。
- ・ISMコードの構造は維持したまま、条文を改廃・集約。マネジメントの要求を定めたうえで、リスク評価に基づき対策群から必要なものを選ぶ構造とした。
- ・会社として何を備えるべきかが要求事項の中で体系立ち、**自社の取組みを全体として見渡せる**。

第1部	第2部 NK CSMS 要求事項		業界要求との対応					
条文	評価基準	客観的証拠	RISQ	DryBMS	SIRE	TMSA	FAL	Rec.194

→ 第1部（条文）の見直し



CSMS ガイドライン | 改訂（2）審査基準の明確化

何を求め、何をもって確認するのかを、第2部として明示した

- ・審査で確認していた内容を、「評価基準」と「求められる客観的証拠」として第2部に整理。
- ・各要求事項について、「評価基準」（満たすべき状態）と「求められる客観的証拠」（何ををもって確認するか）の二つの形で整理。
- ・審査で何を示せば良いのかを事前に把握でき、準備を進めやすい。

第1部	第2部 NK CSMS 要求事項	
条文	評価基準	客観的証拠
会社は、1.2の目的を達成する方策を含むサイバーセキュリティの方針を確立しなければならない	方針が文書化され、目的を達成するための方策と会社としてのコミットメントが示されている。トップマネジメントにより正式に承認されている	方針の文書が存在すること。トップマネジメントによる承認の証拠（署名、承認者及び承認日の記録等）が存在すること

→ 第2部の新設

CSMS ガイドライン | 改訂 (3) CSMSを取り巻く環境の変化への対応

いずれの変化も、それを維持し対応する会社側のマネジメントの重要性に帰着する

課題 ① ベースラインの明確化

UR E26/E27、IACS Rec. 194

- ・船が備えるべき機能について、新造船・就航船それぞれによりどころが示された。
- ・これを維持するため、マネジメントの関与、組織体制、人と教育、手順書の在り方が問われる。

➔ 会社側のガバナンスとマネジメントの重要性はむしろ高まる

課題 ② 参照すべき業界要求の増加

各国の当局

傭船者

荷主

- ・類似した要求がそれぞれ独自の様式で求められている。
- ・本会で読み解いたところ、その多くはマネジメントに関する要求。

➔ 変化の激しい外部要求を読み解き、対魚を整理する作業が積み重なる

CSMS ガイドライン | 改訂（3）CSMSを取り巻く環境の変化への対応

第2部に該当する外部要求を併記し、CSMS一つで対応関係を確認できる形にした

- ・各団体・制度で示される外部要求を本会で整理し、第2部の各要求事項に該当する外部要求を併記。
- ・第一弾として、船主・管理会社にとって足元の課題となっている 以下の4つとの対応関係を反映した。
- ・個別に外部要求を読み解く必要がなく、CSMSを共通の軸として、対応関係を確認できる。

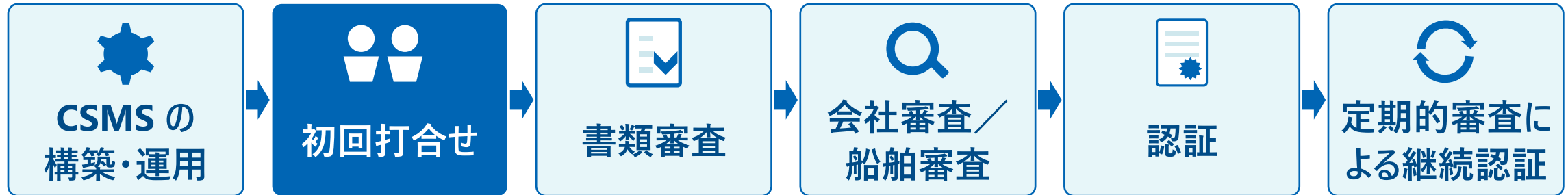
RISQ	ドライバルク船の検査質問票	DryBMS	ドライバルク船の管理基準
SIRE 2.0	タンカーの船舶検査制度	TMSA	タンカー管理の自己評価

第1部	第2部 NK CSMS 要求事項		業界要求との対応					
条文	評価基準	客観的証拠	RISQ	DryBMS	SIRE	TMSA	FAL	Rec.194

→ 各条文に外部要求との対応を併記

CSMS ガイドライン | 認証取得までの流れ

初回打合せで目指す水準を共有し、審査と継続的な改善を同じ方向に進められる



初回打合せで確認すること

- ・トップマネジメントを中心に、現在の取組み状況。
- ・どの外部要求を重視し、対策としてどの程度を目指すのか。

認証取得後

- ・マネジメントに関する要件は、一度満たせば終わりではなく、成熟度を継続的に高めていく分野。
- ・定期的な審査を通じて継続認証となる。

※ 既に認証を取得している会社にも、管理体制を一から見直すことを求めるものではない。

CSMS ガイドライン | まとめ

これまでの取組みをベースに、より使いやすい形に組み直した改訂

改訂点 (1) 国際標準との整合

ISMコードの構造を維持しつつ、**ISO 27001・27002** の体系を踏まえて条文を最新化した。
審査の場で個別に参照していた国際標準を、**要求事項として明確に位置づけた。**

改訂点 (2) 審査基準の明確化

何を求めるのかを、「**評価基準**」と「**求められる客観的証拠**」という形で具体的に示した。
審査で何を示せばよいのかを事前に把握でき、準備を進めやすい。

改訂点 (3) 外部環境の変化への対応

第2部に外部要求を併記し、**CSMS一つで対応状況を確認できる形にした。**
第一弾は **RISQ／DryBMS／SIRE 2.0／TMSA。**

おわりに | 次のステップ

出発点は、自船にとって何が必要かの見極め

本ご紹介した内容

3つのガイドラインを改訂。それぞれの脅威への備えを、Notationまたは認証として示せる。

先進的な安全対策に関するガイドライン

a-SAFE(GIMS)

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

CybR-G(ES)

サイバーセキュリティマネジメントシステムガイドライン

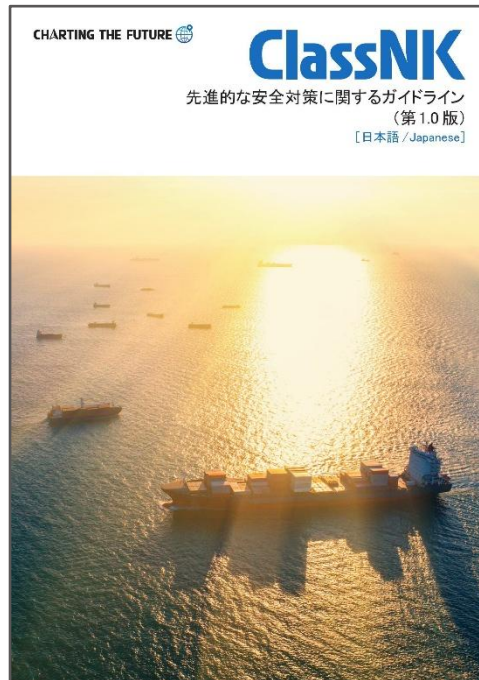
認証

次のステップ

自船の状況に照らし、必要なものから着手できる

おわりに | お問い合わせ

a-SAFE ガイドライン



CybR-G ガイドライン



CSMS ガイドライン



一般財団法人 日本海事協会 船舶管理システム部

TEL : 03-5226-2173 / E-mail : smd@classnk.or.jp



Thank you for your kind attention