船舶サイバーレジリエンス要件への対応

- 船主・船舶管理会社に求められる実務 -

照井／草本
一般財団法人日本海事協会　機関部

目次

IACS*1は、サイバーセキュリティを最低限確保する一対の統一規則を制定

IACS UR E27

「船上のシステム及び機器のサイバーレジリエンス*2 」

システム・機器レベルでのサイバーレジリエンス確保

IACS UR E26

「船舶のサイバーレジリエンス」

船舶全体でのサイバーレジリエンス確保

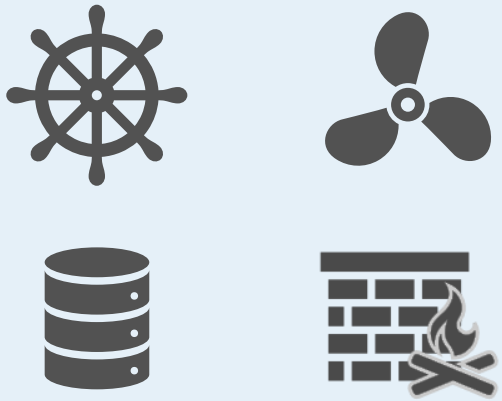
*1 国際船級協会連合：主要な船級協会が加盟する、船舶の設計、建造、運航に関するルールの策定などを行う組織

*2 システム障害やサイバー攻撃が発生しても、機能を維持し、迅速に回復できる能力

IACS UR E27 (Rev.1)

（鋼船規則X編4章）
「船上のシステム及び機器のサイバーレジリエンス」

メーカー（供給者）は、
サイバーレジリエンスを
考慮した機器を供給

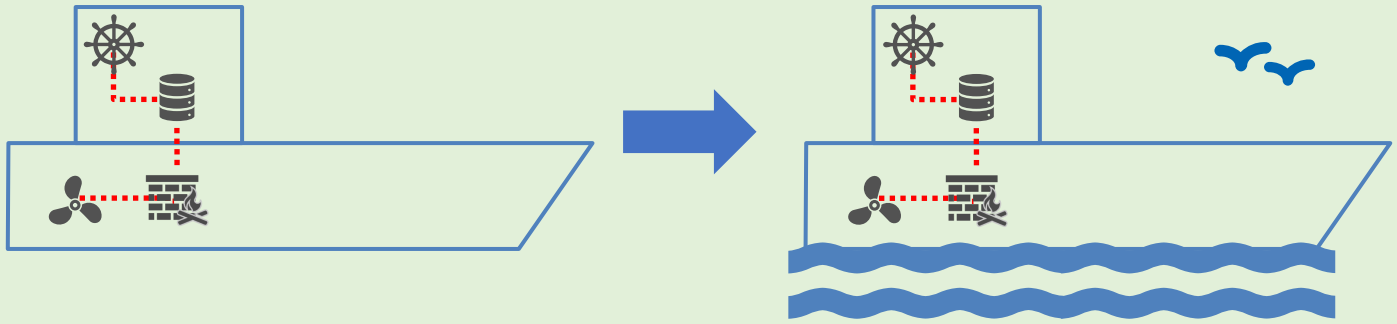


IACS UR E26 (Rev.1)

（鋼船規則X編5章）
「船舶のサイバーレジリエンス」

造船所（統合者）は、
サイバーレジリエンスを
確保した船舶を建造

船主・管理会社は、
就航中の船舶の
サイバーレジリエンスを維持



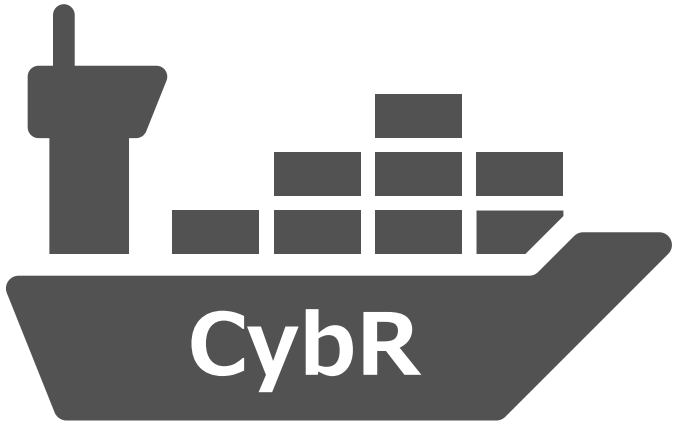
適用対象船舶

2024年7月1日以降に建造契約が行われる船舶のうち、以下に該当する船舶に適用

- 国際航海に従事する旅客船（高速旅客船を含む）
- 総トン数500トン以上の国際航海に従事する貨物船
- 総トン数500トン以上の国際航海に従事する高速船
- 総トン数500トン以上の海洋資源掘削船
- 建設（例えば風力発電設備の保守及び補修，クレーン設備，ドリリングテンダー，居住等）に従事する自航式海洋構造物

💡 **内航船**や**2024年6月30日以前の建造契約の船舶**は**対象外**

ClassNKでは、UR E26/E27の要件に適合する船舶に対して、
完工時に船級符号に「CybR」を付記



2. IACS UR E26の概要

UR E26では、船舶をサイバー攻撃などから守るために必要となる対策を、５つの機能要素に分類

識別　船舶が所有するシステムやネットワーク機器などの資産を**「見える化」**すること

防御　起こりうるサイバーインシデントの**規模と頻度を最小化**すること

検知　**サイバーインシデントを特定**すること

対応　サイバーインシデントを検知した場合**影響を最小化するための手段を構築**すること

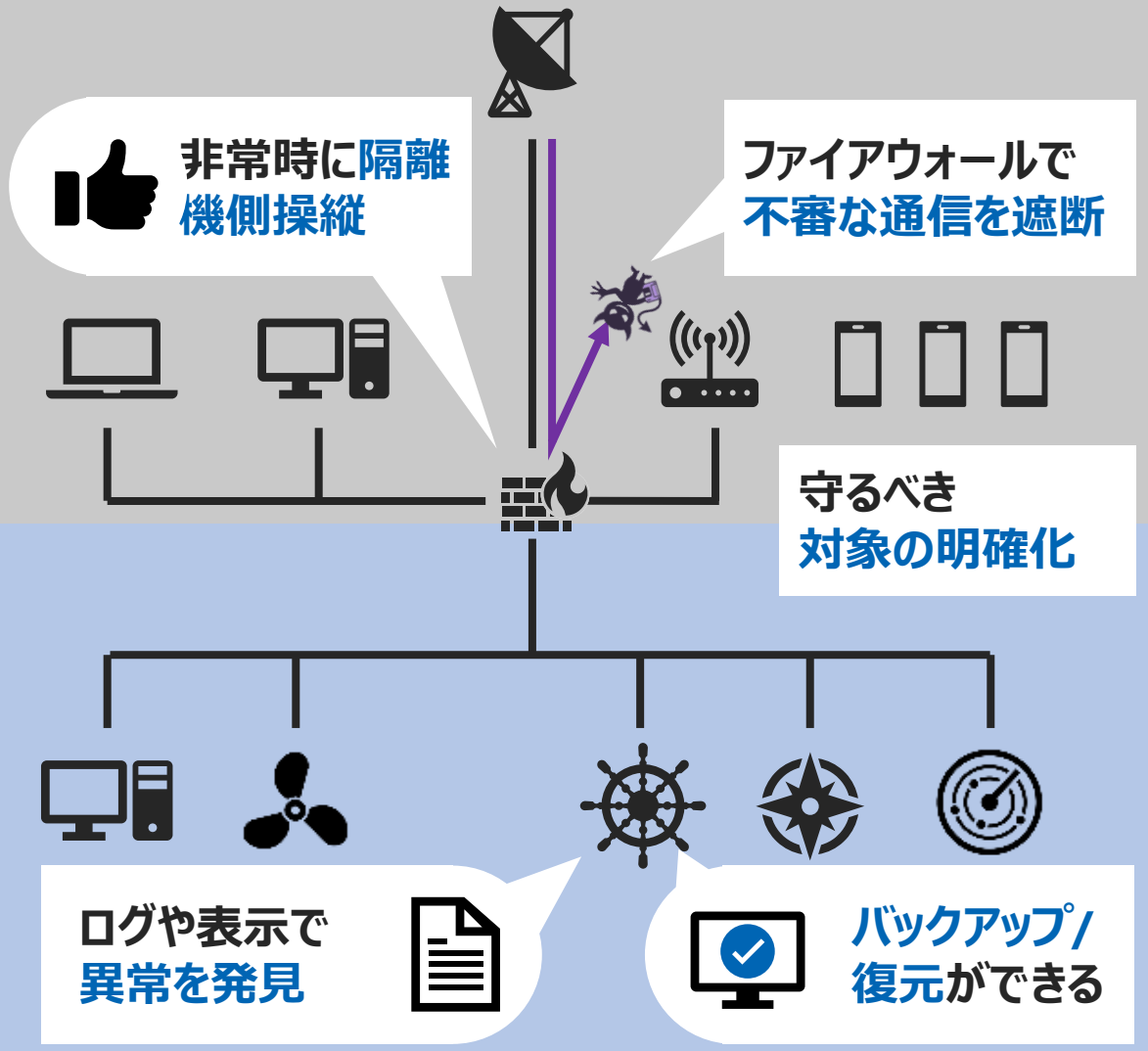
復旧　サイバーインシデントによる混乱又は故障後、**使用可能な状態へ回復**すること

5つの要素の要件を満足することで、船舶のサイバーリスクを軽減し、安全運航を確保

2. IACS UR E26の概要

ClassNK

UR E26(鋼船規則X編)に適合した船舶



識別
- 守るべきシステムを見える化し管理する

防御
- ファイアウォールで不審な通信を遮断する
- 各機器の防御機能も併用する

検知
- 各機器のログや表示で異常を発見する

対応
- 非常時は通信を遮断する
- 機側操縦に移行する

復旧
- バックアップデータで機器を復旧する

船主対応の流れ　～建造契約から初回の年次検査まで～

建造契約　進水　引き渡し　運航開始　初回の年次検査

- ✓ 船主支給品情報を早急に造船所に共有
- ✓「計画書*」の作成・承認
- ✓「計画書」に基づく管理・記録
- ✓「計画書」に基づく記録の提示

*計画書：船舶サイバーセキュリティ・レジリエンス計画書

3. IACS UR E26への船主対応の流れ　~建造契約から進水まで~

ClassNK

E26範囲外

※一例

衛星通信システム

船主支給品も対象

④適用対象外のシステム

Firewall

ITゾーン
(ビジネスLAN)

ビジネスLAN
スイッチ

事務用PC　サーバー　データ監視用PC

ITゾーン
(クルーLAN)

クルーLAN
スイッチ

Firewall

OT LAN
スイッチ

※OT：Operation Technology

OTシステム
（遠隔保守／
遠隔監視）

機関制御装置

発電機御装置

OTゾーン（機関）

データサーバー
（VDR用）

VDR

データサーバー
（ECDIS用）

レーダー

ECDIS

OTゾーン（航海機器）

E26範囲内

①適用対象のOTシステム

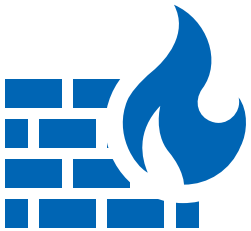
②適用対象のシステムの通信を制御・管理するネットワーク機器

③適用対象のOTシステム以外の、適用対象のシステム

適用範囲におけるポイント

適用対象船舶であるか

⇨建造契約日、総トン数(GT)、航行区域(国際航海の有無)などの確認



船舶のネットワーク構成によって適用範囲が変化

⇨船主支給品のネットワーク構成への影響を造船所と確認・共有

適用範囲内の船主支給品もE27承認取得が必要

⇨適用範囲内の場合はE27承認取得品を手配

船主/管理会社作成資料｜船舶サイバーセキュリティ・レジリエンス計画書

概要　運航中のサイバーレジリエンスの維持・管理のため、船舶の運用ルールを定めた計画書

運用できるようにする

計画書

- 変更管理
- ウイルス対策手段
- 異常検知手段
- 対応計画
- 復旧計画　　など

- ✓ **初回の年次検査までに弊会に提出し、承認を得る必要がある**
- ✓ 年次・中間・定期検査での**計画書の実施記録確認に利用**する
- ✓ **メーカー様、造船所の提出資料**により大部分を作成可能

計画書に記載する主な内容

変更管理

機器・ソフトウェアの変更プロセスを定め、
船舶資産インベントリを最新の状態に維持する。

ウイルス対策手段

マルウェア対策ソフトやUSB等の事前スキャンを実施し、
感染防止と定義ファイルの更新を行う。

異常検知手段

各システムのログや警報を監視し、
不審な通信、システムの異常を早期に把握する。

対応計画

インシデント発生時の連絡、影響範囲の特定、
ネットワーク隔離、機側・手動制御への移行など、
初動手順を定める。

復旧計画

バックアップを用いた復元・再起動の手順、
関係者への連絡、復旧後の正常性確認を定める。

Point　**計画書は「作成して終わり」ではなく、運航中の管理と記録を継続するための手順書です**

3. IACS UR E26への船主対応の流れ　~初回の年次検査まで~

UR E26/E27における提出資料一覧

メーカー
X編4章 (UR E27)

- コンピューターシステム資産インベントリ
- トポロジー図
- セキュリティ機能仕様書
- セキュリティ機能試験要領書
- セキュリティ構成指針
- セキュア開発ライフサイクル文書
- 保守・検証手順書
- インシデント対応・復旧計画支援情報
- 変更管理手順書
- 供給者による試験報告書*

(*型式承認引当て時のみ)

情報提供

造船所
X編5章 (UR E26)

- 船舶資産インベントリ
- ゾーン及びコンジット図
- コンピュータシステムを適用除外とするためのリスク評価
- サイバーセキュリティデザインの説明
- 補完的対策の説明
- 船舶サイバーレジリエンス試験要領書

情報提供

船主/管理会社
X編5章 (UR E26)

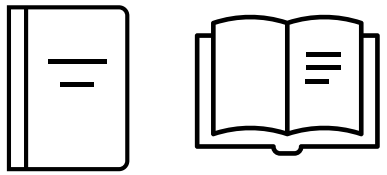
- 船舶サイバーセキュリティ・レジリエンス計画書

3. IACS UR E26への船主対応の流れ　~初回の年次検査まで~

計画書例：ウイルス対策，マルウェア対策，スパム対策及び悪意のあるコードからのその他の防御

[UR E26 4.2.3 (X 編 5.4.3(3))]

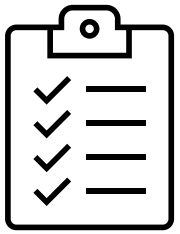
メーカー資料
(又は造船所資料)



マルウェア対策ソフトの保守及びアップデートは、本船の責任者が以下の表に記載の手順に従って管理すること。

CBS	マルウェア対策 ソフトの有無・方式	保守／アップデート手順	デバイスの接続可否
主機制御装置	有 (ホワイトリスト)	Doc.No. AA	不可
発電機制御装置	無	Doc.No. AB	不可
ECDIS	無	Doc.No. AD	可（要スキャン）
VDR	有 (シグネチャー)	Doc.No. AE	可
Firewall	無	Doc.No. AF	不可

船主ポリシー
(管理上の決め事)

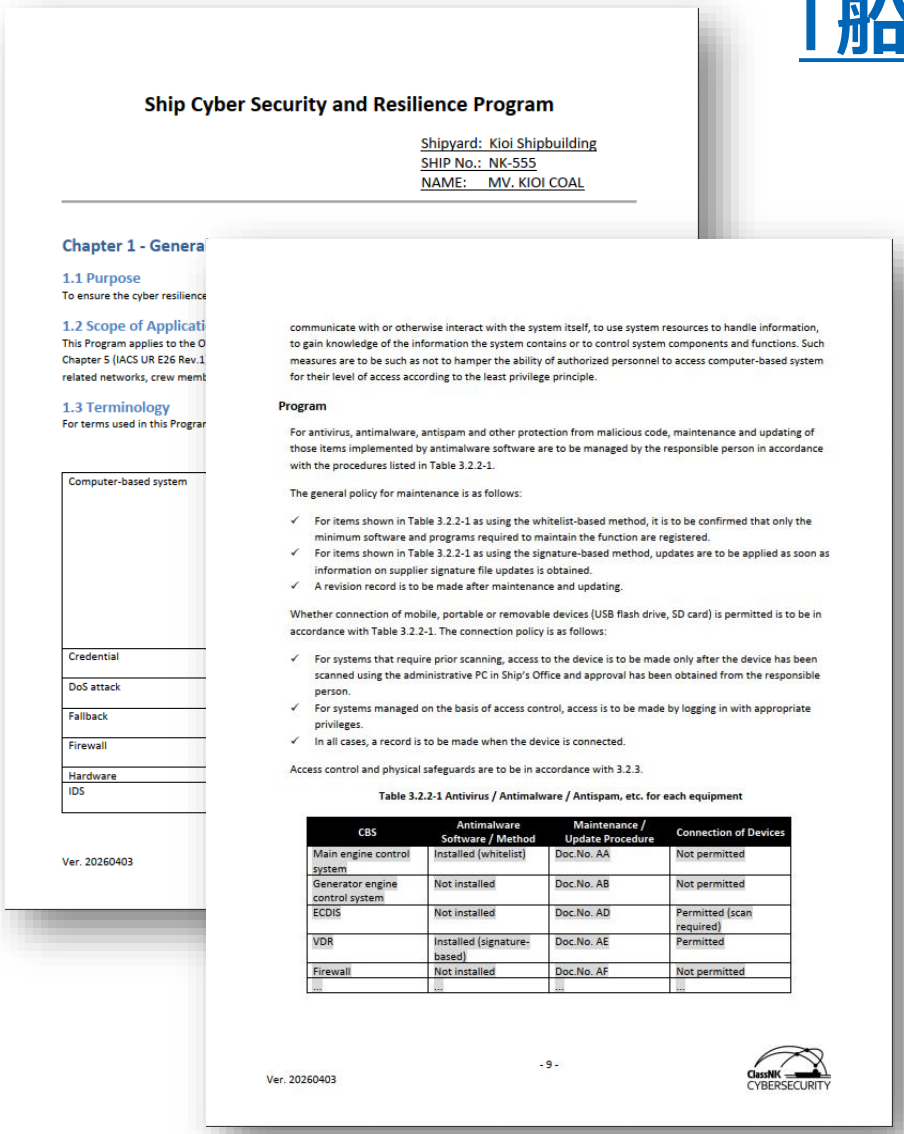


保守に際しての一般的なポリシーの例は、以下によること。

- **アクセス制御に基づく管理がなされているシステムにおいては、管理者A によるログインのうえアクセスすること。**
- 保守及びアップデートの実施後の**更新記録**を取ること。

年次検査で確認する記録

3. IACS UR E26への船主対応の流れ　~初回の年次検査まで~



Ship Cyber Security and Resilience Program

Shipyard: Kioi Shipbuilding
SHIP No.: NK-555
NAME: MV. KIOI COAL

Chapter 1 - Genera

1.1 Purpose
To ensure the cyber resilience

1.2 Scope of Applicati
This Program applies to the O
Chapter 5 (IACS UR E26 Rev.1
related networks, crew memb

1.3 Terminology
For terms used in this Prograr

Computer-based system
Credential
DoS attack
Fallback
Firewall
Hardware
IDS

Ver. 20260403

communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions. Such measures are to be such as not to hamper the ability of authorized personnel to access computer-based system for their level of access according to the least privilege principle.

Program

For antivirus, antimalware, antispam and other protection from malicious code, maintenance and updating of those items implemented by antimalware software are to be managed by the responsible person in accordance with the procedures listed in Table 3.2.2-1.

The general policy for maintenance is as follows:

- ✓ For items shown in Table 3.2.2-1 as using the whitelist-based method, it is to be confirmed that only the minimum software and programs required to maintain the function are registered.
- ✓ For items shown in Table 3.2.2-1 as using the signature-based method, updates are to be applied as soon as information on supplier signature file updates is obtained.
- ✓ A revision record is to be made after maintenance and updating.

Whether connection of mobile, portable or removable devices (USB flash drive, SD card) is permitted is to be in accordance with Table 3.2.2-1. The connection policy is as follows:

- ✓ For systems that require prior scanning, access to the device is to be made only after the device has been scanned using the administrative PC in Ship's Office and approval has been obtained from the responsible person.
- ✓ For systems managed on the basis of access control, access is to be made by logging in with appropriate privileges.
- ✓ In all cases, a record is to be made when the device is connected.

Access control and physical safeguards are to be in accordance with 3.2.3.

Table 3.2.2-1 Antivirus / Antimalware / Antispam, etc. for each equipment

CBS	Antimalware Software / Method	Maintenance / Update Procedure	Connection of Devices
Main engine control system	Installed (whitelist)	Doc.No. AA	Not permitted
Generator engine control system	Not installed	Doc.No. AB	Not permitted
ECDIS	Not installed	Doc.No. AD	Permitted (scan required)
VDR	Installed (signature-based)	Doc.No. AE	Permitted
Firewall	Not installed	Doc.No. AF	Not permitted
...	...	...	...

Ver. 20260403

- 9 -

ClassNK CYBERSECURITY

「船舶サイバーセキュリティ・レジリエンス計画書サンプル」

- 弊会の顧客が計画書を効率的に作成することを支援
- 以下に情報を追加することで完成
  - 船主のセキュリティポリシー
  - メーカー、造船所資料への参照

本サンプルに関して具体的なご質問がございましたら、ぜひお気軽にご連絡ください。

ClassNK Academy : 海事サイバーセキュリティ　現在公開中！

■船舶内の職員及び陸上の他の関係職員に対して訓練を実施しなければならない

UR E26 5.3　(鋼船規則X編　2.2.3-5(4))

eラーニング : 海事サイバーセキュリティ

- 船上基礎コース – 船員向け –
- 船上上級コース – 管理者向け –
- CSMS (Cyber Security Management System) 構築編
- 技術コース – サイバー攻撃対策編 –

ClassNK Academy : IACS UR E26向けトレーニング

Coming soon!

目的　UR E26の要求事項を理解し、適切に運用するための知識を習得する。

対象　船主、船舶管理会社、船員

eラーニング：IACS UR E26向けトレーニング

船主対応の流れ　～初回の年次検査以降～

建造契約

進水

引き渡し

運航開始

初回の年次検査

✓ 船主支給品情報を
早急に造船所に共有

✓「計画書*」の作成・承認
✓「計画書」に基づく管理・記録

✓「計画書」に基づく記録
の提示

4. 検査

初回の年次検査

検査では、
承認済**計画書の実施記録**を提示

年次・中間検査

検査員が必要と判断した場合に限り
（例えば、計画書またはコンピュータシステムに対して変更があった場合）、
計画書の実施記録を確認

定期検査

(年次・中間の内容に加えて実施)

試験要領書に基づく**試験の実施**
> 一部を除く試験は、検査員判断で**省略可**
> コンピュータシステムが定期検査までに**変更された場合の追加項目有**

＋年次・中間検査の内容

4. 検査

初回の年次検査

検査では、
承認済**計画書の実施記録**を提示

年次・中間検査

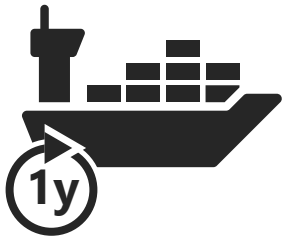
検査員が必要と判断した場合に限り
（例えば、計画書またはコンピュータシステムに対して変更があった場合）、
計画書の実施記録を確認

定期検査

(年次・中間の内容に加えて実施)

試験要領書に基づく**試験の実施**
> 一部を除く試験は、検査員判断で**省略可**
> コンピュータシステムが定期検査までに**変更された場合の追加項目有**

＋年次・中間検査の内容



年次/中間/定期検査における書類確認

以下の要件に基づく計画書上の作成書類の確認

初回は必須、2回目以降は船級判断で**省略**

識別	船舶資産インベントリ - 変更管理、ソフトウェアアップデート
防御	セキュリティゾーン及びネットワークセグメント
	ウイルス対策，マルウェア対策，スパム対策及び悪意のあるコードからのその他の防御
	アクセス制御
	遠隔アクセスの制御及び信頼できないネットワークとの通信
	携帯用及び可搬式デバイスの使用
検知	ネットワーク動作の監視
	コンピュータシステム及びネットワークの検証及び診断機能
対応	インシデント対応計画書
復旧	復旧計画書

計画書アップデートの実施確認

コンピュータシステムや計画書に変更があった場合

計画書の変更	・船舶サイバーセキュリティ・レジリエンス計画書の提出・再承認
	・船舶サイバーセキュリティ・レジリエンス計画書の変更箇所に関する検査

4. 検査

初回の年次検査

初回の年次検査までに弊会機関部へ
計画書を提出・承認取得

検査では、
承認済**計画書に基づく記録**を提示

年次・中間検査

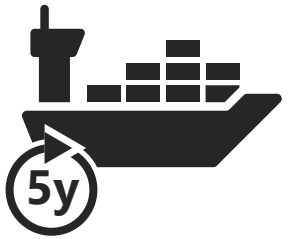
承認済**計画書に基づく記録**を提示
ただし、要否は検査員判断

計画書またはコンピュータシステムに対して
変更があった場合、
変更管理の実施記録を確認

定期検査
(年次・中間の内容に加えて実施)

試験要領書に基づく**試験の実施**
> 一部を除く試験は、船級判断で**省略可**
> コンピュータシステムが定期検査までに
変更された場合の追加項目有

＋年次・中間検査の内容



定期検査における立会試験

定期検査において毎回実施

識別 船舶資産インベントリ

防御 セキュリティゾーン及びネットワークセグメント

ウイルス対策，マルウェア対策，スパム対策及び悪意のあるコードからのその他の防御

遠隔アクセスの制御及び信頼できないネットワークとの通信

携帯用及び可搬式デバイスの使用

省略される項目
(システムの変更により本会が要請した場合実施)

防御 無線通信

ネットワークを防御する防護策

検知 ネットワーク動作の監視

対応 機側、独立及び／又は手動の動作

ネットワークの隔離

ミニマルリスクコンディションへのフォールバック

復旧 バックアップ及び復元の機能

制御されたシャットダウン、リセット、ロールバック及び再起動

- ✓ 通常、**造船所作成の「船舶サイバーレジリエンス試験要領書」**に基づき、**左側の項目を実施**
- ✓ **システムに変更**があった場合、**試験要領書を改正し、右側の項目を追加で実施**

UR E26における 船主/管理会社の主な対応事項

- 造船所への船主支給品情報の早期共有 (暫定的なものでOK)

  ※対象船舶(建造契約日、総トン数、航行区域)をご確認ください (スライド5参照)

- 初回の年次検査までに「計画書」の承認が必要

  ※NK船向けに、「計画書サンプル」をご用意しています

- 「計画書」に基づく年次検査における実施記録の提示
- 「試験要領書」に基づく定期検査における試験の実施

情報収集から実務対応まで、ポータルサイトに集約

IACS UR E26 / E27 の確認に必要な資料へ、ひとつの入口からアクセスできます。

ClassNK サイバーレジリエンス・ポータル

ポータルサイトを開く ➢

ガイドライン
規則要求を実務目線で解説
規則の理解

Q&A
代表的な疑問と回答を検索
判断の補助

解説動画
船主・造船所・メーカー向け
短時間で把握

資料は随時更新 | 最新情報はポータルで確認

ClassNK CHARTING THE FUTURE

Thank you for your kind attention