NKサイバーセキュリティ関連規則の現状説明

NKサイバーセキュリティワークショップ（5月29日広島会場）

NKサイバーセキュリティ関連規則の現状説明

改正の背景

コンピュータシステムの増加
（電子制御機関，船陸間通信等）

サイバー攻撃の巧妙化
（愉快犯⇒金銭目的の犯罪組織，政治目的のテロリスト）

サイバーリスクの高まり

IACS 統一規則　E26「船舶のサイバーレジリエンス」
E27「船上のシステム及び機器のサイバーレジリエンス」

- 適用対象船舶の限定（国際500GT以上の貨物船等）
- 検査要件の明確化
- 業界からのフィードバックの反映

E26 (Rev.1)（2023年11月）
E27 (Rev.1)（2023年9月）

NK規則に取入れ

NKサイバーセキュリティ関連規則の現状説明

改正の背景

IACS Cyber Systems Panel

NKを含む各メンバー船級協会

IACS Joint Working Group / Cyber Systems

船主等：BIMCO, DCSA, ICS, INTERCARGO, INTERTANKO, WSC 等

造船所：ASEF（日本造船工業会を含む）, SeaEurope

製造者：SSAP（日本舶用工業会「スマナビ研」）, CIRM（舶用通信機器製造者等）(, SeaEurope)

保険等：IUMI, International Group of P&I Clubs

IACS 統一規則 E26「船舶のサイバーレジリエンス」
E27「船上のシステム及び機器のサイバーレジリエンス」

NKサイバーセキュリティ関連規則の現状説明

改正内容

IACS 統一規則 E27
「船上のシステム及び機器のサイバーレジリエンス」

（鋼船規則X編4章へ）

⇒詳細：スライド15～16

IACS 統一規則 E26
「船舶のサイバーレジリエンス」

（鋼船規則X編5章へ）

⇒詳細：スライド17～19

IEC 62443シリーズを参考に規定

↑ 産業用オートメーション及び制御システムのサイバーセキュリティを確保するための国際規格

（例）ユーザーの認証，
必要最小限の権限の付与，
携帯用デバイスの使用の管理，
イベントの日時の記録，
システムのバックアップ

既存の複数のガイドライン等を参考に規定

↑ IACS Rec 166，各船級協会のガイドライン，BIMCOガイドライン，NIST SP 800-53等

NIST Frameworkの5要素に分けて要件を整理

（例）識別：「船舶資産インベントリ」の保持
防御：セキュリティゾーンへの分離
検知：ネットワーク動作の監視
対応：「インシデント対応計画書」の保持
復旧：バックアップ及び復元の機能

https://www.nist.gov/cyberframework

（BIMCO：The Baltic and International Maritime Council／ボルチック国際海運協議会
NIST：National Institute of Standards and Technology／アメリカ国立標準技術研究所）

改正内容

IACS 統一規則 E27
「船上のシステム及び機器のサイバーレジリエンス」

（鋼船規則X編4章へ）

⇒詳細：スライド15～16

製造者は，各機器のセキュリティ機能を確保

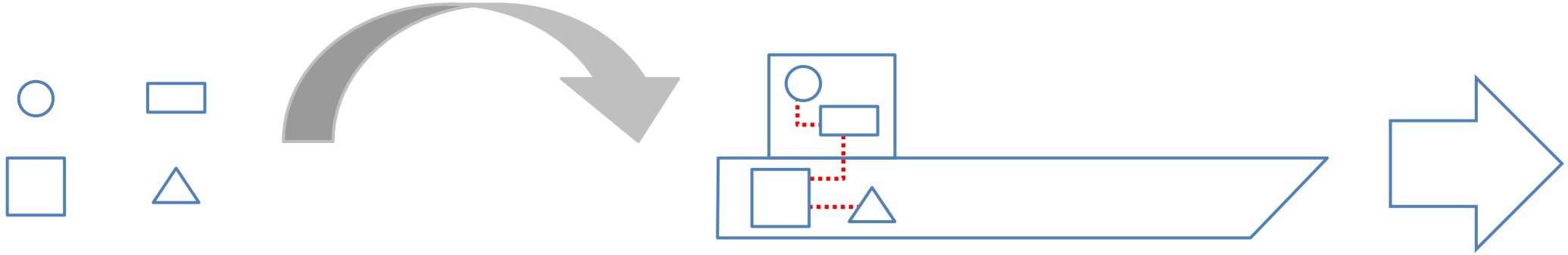
IACS 統一規則 E26
「船舶のサイバーレジリエンス」

（鋼船規則X編5章へ）

⇒詳細：スライド17～19

造船所は，船全体のネットワークを構築

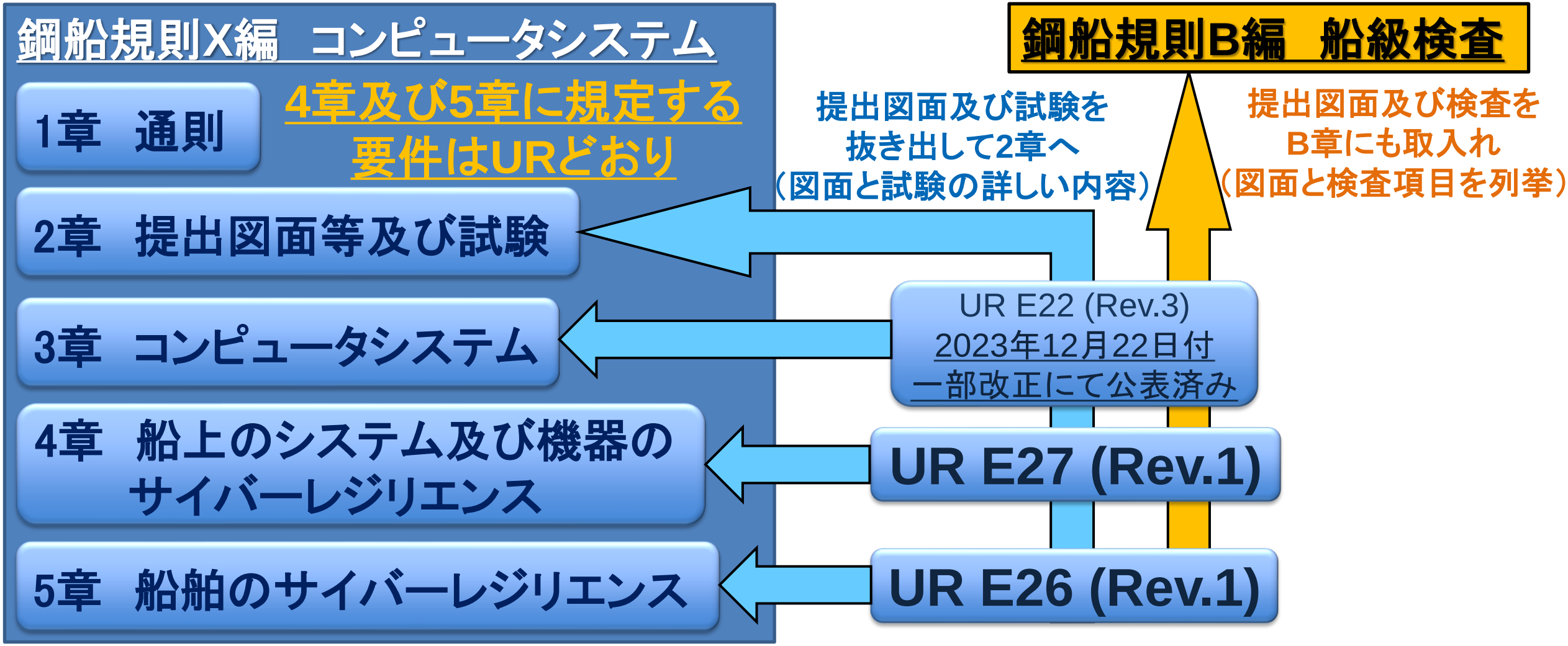
船主は，就航後の運用及びアップデート



（現存船における対策については，IACSにて Recommendation 作成作業中）

改正内容

E27とE26のNK規則への取入れ



NKサイバーセキュリティ関連規則の現状説明

改正内容

鋼船規則 A編：適合船に**船級符号への付記／Notation“Cyber Resilience”**（略号：CybR）
⇒**詳細：スライド9**
B編：**登録検査，年次・中間・定期検査の概要**（X編を参照。年次・中間は書類確認）
⇒**詳細：スライド8**
X編：**2章「提出図面等及び試験」**（3～5章に対応する検査に関する規定）
⇒**詳細：スライド12～14**
3章「コンピュータシステム」（2023年12月22日付 一部改正にて公表済み）
4章「船上のシステム及び機器のサイバーレジリエンス」新設（UR E27より）
⇒**詳細：スライド15～16**
5章「船舶のサイバーレジリエンス」新設（UR E26より）
⇒**詳細：スライド17～19**

船用材料・機器等の承認及び認定要領　第7編「制御及び計装用機器並びに電気設備」
10章「サイバーレジリエンスに関する対策が講じられる機器等の使用承認」新設：
旗国による航海設備等のType Approval（必須）と異なる，任意の承認。
承認を受けると，製造工場等における本会検査を軽減可。（UR E27より）

その他の規則：鋼船規則X編の新規制定に伴う，同編を参照する文言の追加等。

改正内容　鋼船規則B編「船級検査」⇒ 統合者，船主に関連

2章　登録検査

2.1.6 「船上に保持すべき図面等」

鋼船規則X編5章に規定する，船上での検査に必要な図面を追加

3章　年次検査

3.9「船級符号に“CybR”の付記を有する船舶の特別要件」

- **鋼船規則X編5章**に規定する年次検査の要件を追加
- 船上に保持すべき図面として，「船舶サイバーセキュリティ・レジリエンス計画書」を規定
- 表B3.12を作成して確認事項を列挙

①「初回の年次検査」

⇒文書により，10個の要件を確認

②「2回目以降の年次検査」

⇒本会が必要と認める場合に①を実施

4章　中間検査

4.9「船級符号に“CybR”の付記を有する船舶の特別要件」

- **鋼船規則X編5章**に規定する中間検査の要件を追加

⇒実質②「2回目以降の年次検査」と同じ

5章　定期検査

5.9「船級符号に“CybR”の付記を有する船舶の特別要件」

- **鋼船規則X編5章**に規定する定期検査の要件を追加
- 表B5.32にを作成して検査事項を列挙

⇒「船舶サイバーレジリエンス試験要領書」に従って，検査員立会のもと試験を実施

改正内容　鋼船規則X編4章及び5章の適用対象船舶

- 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）に従事する自航移動式洋上船

改正内容　鋼船規則A編1.2.4-35. 船級符号の付記

X編4章及び5章の適用を受けた，サイバーレジリエンスに関する対策が講じられる船舶については，船級符号に“Cyber Resilience”（略号 CybR）を付記する。

改正内容

鋼船規則X編4章及び5章の適用対象システム

- **推進**
- **投錨**及び**係留**
- **発電**及び**分電**
- **火災探知**及び**消火システム**
- **ビルジ**及び**バラストシステム**、**積付計算機**
- **水密性**及び**浸水検知**
- **照明**（例えば、非常灯、低位置、航海灯等）
- **安全が要求されるシステム**であって、当該システムの混乱又は機能障害が船舶の運航にリスクをもたらしうるもの（例えば、緊急停止システム、荷役安全システム、圧力容器安全システム及びガス検知システム等）
- 条約により要求される**航海設備**
- 船級規則又は条約により要求される**船内及び船外通信システム**
- **その他**（自動船位保持設備など）

改正内容 鋼船規則X編4章及び5章における，利害関係者の定義

船主/会社：

船舶の所有者又は当該所有者から船舶の運用に関する責任を引き受け，かつ，すべての付随する義務及び責任を引き受けることに合意した管理者，代理人又は裸傭船者のような組織若しくは人をいう。新造時において，船主は，造船所又は統合者であることがある。船舶の引渡し後，船主は責任の一部を船舶管理会社に委託することができる。

供給者：

アプリケーション，埋め込みデバイス，ネットワークデバイス，ホストデバイス等であって全体としてシステム又はサブシステムとして機能するものから成る，ハードウェア及び／又はソフトウェア製品，システムコンポーネント又は機器（ハードウェア若しくはソフトウェア）の製造者又は提供者をいう。船舶引き渡し後，供給者は，プログラム可能なデバイス，サブシステム又はシステムを，統合者に提供することに責任を有する。

統合者：

供給者から提供されるシステム及び製品を，船舶の仕様による要求に合ったシステムへ統合すること及び統合されたシステムを提供することに対して責任を有する特定の個人又は組織をいう。統合者は，船内におけるシステムの統合にも責任を有することがある。この役割は，船舶を引き渡すまでは，他の組織がこの責任について特に契約／指定される場合を除き，造船所によって担われなければならない。

NKサイバーセキュリティ関連規則の現状説明

改正内容　鋼船規則X編2章　提出図面等及び試験

4章：船上のシステム及び機器
5章：船舶

2.1.1「提出図面及び資料」

- 両URに規定される，提出図面及び資料

2.2.2「4章における試験」

- UR E27(Rev.1)に規定される，**供給者**が実施する製造工場等における試験

2.2.3「5章における試験」

- UR E26(Rev.1)に規定される，**統合者**又は**船主**が実施する，要件への適合を実証するための試験について規定

表X2.3「4章に関する，供給者による提出資料の概要」

- UR E27(Rev.1)に規定される資料と各要件との対応
- 各資料が参考用／承認用のどちらであるか
- **使用承認**を受けた場合に，提出すべき資料

表X2.4「5章に関する，統合者又は船主による提出資料の概要」

- UR E27(Rev.1)に規定される資料について，誰が，いつ，何をすべきか

表X2.5「5章に関する要件及び図書の概要」

- UR E26(Rev.1)に規定される，各要件に関連する資料とその関連規則

改正内容

表X2.3「4章に関する，供給者による提出資料の概要」

表 X2.3 船上のシステム及び機器のサイバーレジリエンスに関する，供給者による提出資料の概要

番号	提出資料（参照規則）	要件（参照規則）	参考	承認
1	コンピュータシステム資産インベントリ (4.4.1(1))	インベントリ (5.4.2(1))	-	○(1), (2)
2	トポロジー図 (4.4.1(2))	システムの図書 (5.4.3(1))	-	○(1), (2)
3	セキュリティ機能仕様書 (4.4.1(3))	要求されるセキュリティ機能 (4.4.2) 追加で要求されるセキュリティ機能（該当する場合）	-	○(1)
⋮				
9	変更管理手順書 (4.4.1(9))	手順の変更に関する管理 (3章)	○(1)	-
10	供給者による試験報告書 (4.4.1(10))	セキュリティ機能の設定及びハードニング (4.4.1(5)及び4.5.8)	○(2)	-

（備考）
承認：承認用図面及び資料
参考：参考用図面及び資料
(1)：船用材料・機器等の承認及び認定要領第7編10章に従って使用承認を受けていない場合に提出
(2)：船用材料・機器等の承認及び認定要領第7編10章に従って使用承認を受けた場合に提出

提出資料に関連する規則の参照先

提出資料の詳細を規定している規則の参照先

使用承認を受けた場合に提出するか否かを添え字で記載

改正内容

表X2.4「5章に関する，統合者又は船主による提出資料の概要

表 X2.4 船舶のサイバーレジリエンスに関する，統合者又は船主による提出資料の概要

番号	提出資料（参照規則）	統合者			船主			
		設計時	建造中	試運転	就航後	初回年次	年次・中間	定期
1	承認された供給者の文書（2.2.3）	-	保守	保守	保守	-	-	-
2	ゾーン及びコンジット図（2.2.3-3.(4)）	提出	保守	保守	保守	-	-	-
3	サイバーセキュリティデザインの説明（2.2.3-3.(5)）	提出	保守	保守	保守	-	-	-
：								
-	復旧計画（5.4.6(1)(d)iv））							

各資料について，
誰が，いつ，何をすべきか

提出資料に関連する規則の参照先

（備考）

*：該当する場合に限る。

提出：利害関係者は，5 章に規定する要求事項への適合の検証及び承認のために，本会に文書を提出しなければならない。

保守：利害関係者は，変更管理の手順に従って文書をアップデートし続けなければならない。アップデートされた文書及び変更管理記録は，表 X2.2 に従って本会に提出されなければならない。

実証：利害関係者は，承認された文書に従って，本会に対して適合を実証しなければならない。

初回年次：初回の年次検査

年次・中間：2 回目以降の年次検査

定期：定期検査

何をすべきかの詳細

NKサイバーセキュリティ関連規則の現状説明

改正内容

鋼船規則X編4章⇒ 供給者に対する要件
「船上のシステム及び機器のサイバーレジリエンス」

4.1 一般
4.2 定義及び略語の説明
4.3 セキュリティの考え方
- **不可欠なシステムの可用性**
  ⇒セキュリティ対策により，安全機能，制御機能，監視機能等が喪失してはならない
- **補完的対策**
  ⇒本来のセキュリティ機能に代えて補完的対策を取ることも可

4.4 船上のシステム及び機器のサイバーレジリエンスの要件
4.4.1 船上のシステム及び機器のサイバーレジリエンスに関わる提出資料（10個）
4.4.2 要求されるセキュリティ要件（30個）
⇒適用範囲内にあるすべてコンピュータシステムに対して要求
4.4.3 追加で要求されるセキュリティ要件（11個）
⇒信頼できないネットワーク（適用範囲外にあるすべてのネットワーク）とのネットワーク通信を行うコンピュータシステムに対して要求
4.5 セキュア開発ライフサイクルに関する要件
⇒システム又は機器を開発するにあたり，開発中の全ての段階におけるセキュリティ面の取り扱いを文書化
4.6 適合の実証

NKサイバーセキュリティ関連規則の現状説明

改正内容

鋼船規則X編4章⇒ 供給者に対する要件
「船上のシステム及び機器のサイバーレジリエンス」

4.3.4「補完的対策」
セキュリティ要件を満たすために，**本来のセキュリティ機能に代えて又は加えて，補完的対策を採用することができる**。補完的対策は，参照する規格を考慮し，また，各要件と規格の関連項目との差異を考慮し，**4.4.1(3)に規定する原則に従って**，元々規定されている要件の目的及び厳しさを満足しなければならない。

補完的対策を採用する場合，
セキュリティ機能仕様書にその旨を記載して本会へ提出

4.4.1(3)「セキュリティ機能仕様書」（4章に関する提出資料の3番目）
(e) 要求事項に完全に準拠していない場合，その旨を記載し，補完的対策を提案しなければならない。補完的対策は，次のとおりとする。
i) 元々規定されている要件と同じ脅威から保護すること。
ii) 元々規定されている要件と同等の厳しさ，正確さであること。
iii) 本章の他の要求事項により要求されるセキュリティ管理ではないこと。
iv) 新たなセキュリティリスクを発生させないこと。

補完的対策の例

【要件】表X4.1中10
「可搬式及び携帯用デバイスの使用の管理」
A) 使用は，設計上許可されたものだけに制限すること
B) コード及びデータの転送を制限すること

【補完的対策】
- ポートをブロッカーによりブロックする
- 使用前にデバイスをクリーンナップする等

NKサイバーセキュリティ関連規則の現状説明

改正内容

鋼船規則X編5章⇒ 統合者，船主に対する要件
「船舶のサイバーレジリエンス」

5.1 一般
5.2 定義
5.3 目的及び要件の詳細
5.4 船上のサイバーレジリエンスの要件
5.4.1 一般
5.4.2 識別（1個）
5.4.3 防御（7個）
5.4.4 検知（2個）
5.4.5 対応（4個）
5.4.6 復旧（3個）
5.5 コンピュータシステムを要件の適用対象から除外するためのリスク評価
⇒リスク評価を行い，リスクレベルが許容範囲内であることを示すことで，要件の適用対象から除外することができる

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf

改正内容

鋼船規則X編5.4⇒ 統合者，船主に対する要件

「各セキュリティ要件の構成」

(a) 要件
(b) 根拠
(c) 要件の詳細
具体的な要件の内容
(d) 適合のための実証
i) 設計段階
ii) 建造段階
iii) 試運転段階
iv) 運用段階
1) 一般要件
2) 初回の年次検査
3) 2回目以降の年次検査
4) 定期検査

重要なのはここ

(d) 適合のための実証
作成すべき資料の詳細及び実施すべき試験の詳細を各段階で規定

i) ii) iii) → **統合者が実施**

iv) 1) 2) 3) 4) → **船主が実施**

NKサイバーセキュリティ関連規則の現状説明

改正内容

鋼船規則X編5.5⇒ 統合者が提出し，船主が保守
「コンピュータシステムを要件の適用対象から除外するためのリスク評価」

「リスク評価」

以下の要素を考慮

(1) 資産の脆弱性
(2) 内的及び外的脅威
(3) サイバーインシデントが，人員及び船舶の安全等に及ぼす潜在的な影響
(4) システムの統合又はシステム間のインターフェースに関連する影響

「合格基準」

規準を全て満たしていない場合にも，証拠とともに合理的な説明が提供されれば，当該除外を受け入れることがある。

- 隔離する（他のシステムやネットワークへのIPネットワーク接続がない）
- アクセス可能な物理的インターフェースポートを持たない
- 物理的なアクセスが制御されているエリアに配置する等

統合者は，システムを適用除外とする場合，リスク評価を実施し，
「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」を本会へ提出

「保守」

- 船主は，船舶の運用期間中，継続的な改善のプロセスにおいて，リスク評価を最新の状態にアップデート
- 新たなリスクが特定された場合，既存のリスク低減措置をアップデートするか，新たなリスク低減措置を実施
- サイバーシナリオの変更により，サイバーリスクが許容可能なリスク閾値を超える場合，本会に通知し，アップデートされたリスク評価を提出

NKサイバーセキュリティ関連規則の現状説明

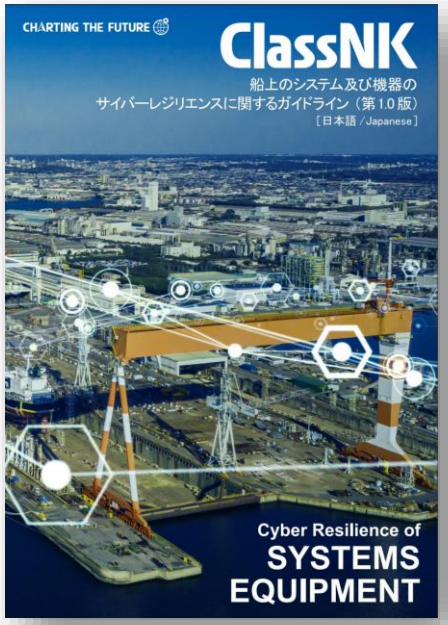
4章　船上のシステム及び機器のサイバーレジリエンス (E27(Rev.1)の取入れ)

5章　船舶のサイバーレジリエンス（E26(Rev.1)の取入れ）

船上のシステム及び機器のサイバーレジリエンスに関するガイドライン

2023年11月2日発行済

- 具体的な適用対象
- 承認プロセスの説明
- 要件の解説
- 書類審査及び立会検査における具体的な確認項目
- 使用承認に関する解説等



船舶のサイバーレジリエンスに関するガイドライン

2024年発行予定

- 具体的な適用対象
- 要件の解説
- 書類審査及び立会検査における具体的な確認項目
- リスク評価による適用除外に関する解説等

- UR E27 (Rev.1)を取入れた，鋼船規則X編4章の内容をガイドラインにて補足
- UR E26 (Rev.1)を取入れた，鋼船規則X編5章についてもガイドライン作成中
- ガイドラインは，鋼船規則を参照し，それぞれの要件に対応している

施行日

2024年7月１日以降に建造契約が行われる船舶に適用