目次

鋼船規則 X 編　　コンピュータシステム

1 章　　通則

1.1　　一般

1.1.1　　適用

本編の規定は，コンピュータシステムに適用する。適用対象の詳細については，**3 章**以降の各章の規定による。

1.1.2　　同等効力

本編の規定に適合しないコンピュータシステムであっても，本会が本編の規定に適合するものと同等の効力があると認める場合には，これを本編に適合するものとみなす。

2章　提出図面等及び試験

2.1　提出図面等

2.1.1　提出図面及び資料

提出すべき図面及び資料は，一般に次のとおりとする。

(1) 承認用図面及び資料

(a) **3章**の適用を受けるコンピュータシステムに関して，当該コンピュータシステムの分類ごとに **2.2.1** の各項に規定する，承認用図面及び資料。その概要を，**表 X2.1** 及び**表 X2.2** に示す。なお，**船用材料・機器等の承認及び認定要領第 7 編 8 章**の規定により使用承認を受けたコンピュータシステムについては，当該使用承認を受けた際の図面及び資料によることができる。

(b) **4章**の適用を受けるコンピュータシステムに関して，**4.4.1(1), (2), (3), (4)**及び**(6)**に規定する，承認用資料。その概要を，**表 X2.3** に示す。ただし，**船用材料・機器等の承認及び認定要領第 7 編 10 章**の規定により既に使用承認を受けたコンピュータシステムについては，**4.4.1(1)**に規定する「コンピュータシステム資産インベントリ」及び **4.4.1(2)**に規定する「トポロジー図」を除き，**4.4.1(10)**に規定する「供給者による試験報告書」を提出した上で，当該使用承認を受けた際の図面及び資料によることができる。

(c) **5章**の適用を受けるコンピュータシステムに関して，**2.2.3-3.(4), (5), (6), (7)**及び**(8)**並びに **2.2.3-4.(2)**規定する，承認用図面。また，**5章**に関連する提出資料の提出者及び提出資料の概要を**表 X2.4** に，**5章**の各要件について関連する資料の概要を**表 X2.5** にそれぞれ示す。

(d) その他本会が必要と認める図面及び資料

(2) 参考用図面及び資料

(a) **3章**の適用を受けるコンピュータシステムに関して，当該コンピュータシステムの分類ごとに **2.2.1** の各項に規定する，参考用図面及び資料。その概要を，**表 X2.1** 及び**表 X2.2** に示す。ただし，**船用材料・機器等の承認及び認定要領第 7 編 8 章**の規定により使用承認を受けたコンピュータシステムについては，**2.2.1-3.(3)**に規定する「コンピュータシステムの分類の一覧」を除き，当該使用承認を受けた際の図面及び資料によることができる。

(b) **4章**の適用を受けるコンピュータシステムに関して，**4.4.1(5), (7), (8)**及び**(9)**に規定する，参考用資料。その概要を，**表 X2.3** に示す。ただし，**船用材料・機器等の承認及び認定要領第 7 編 10 章**の規定により既に使用承認を受けたコンピュータシステムについては，**4.4.1(10)**に規定する「供給者による試験報告書」を提出した上で，当該使用承認を受けた際の図面及び資料によることができる。

(c) その他本会が必要と認める図面及び資料

表 X2.1　　システム供給者による提出資料の概要（3 章「コンピュータシステム」関連）

番号	参照規則	提出資料	分類I		分類 II 及び III	
			参考	承認	参考	承認
1	**2.2.1-2.(1)**及び **3.4.2-1.**	品質計画書及び品質マニュアル	-	-	-	○
2	**2.2.1-2.(3)**及び **3.4.2-3.**	システムの仕様書及び設計書	○*	-	-	○
3	**2.2.1-2.(4)**及び **3.4.2-4.**	環境への適合性を示す資料	○*	-	○	-
4	**2.2.1-2.(5)**及び **3.4.2-5.**	ソフトウェア試験の試験報告書	-	-	○*	-
5	**2.2.1-2.(6)**及び **3.4.2-6.**	システム試験の試験報告書	-	-	○*	-
6	**2.2.1-2.(7)**及び **3.4.2-7.**	FAT の試験方案	-	-	-	○
7	**2.2.1-2.(7)**及び **3.4.2-7.**	FAT の試験報告書	-	-	○	-
8	**2.2.1-2.(7)**及び **3.4.2-7.**	FAT の追加資料 (ユーザーマニュアル等)	-	-	○*	-
9	**2.2.1-2.(8)**及び **3.4.2-8.**	変更管理手順書	-	-	-	○

（備考）

承認：承認用図面及び資料

参考：参考用図面及び資料

○：提出

○*：本会／本会検査員が必要と認める場合に提出

システムの分類については **3.3.1** を参照

表 X2.2　　統合者による提出資料の概要（3 章「コンピュータシステム」関連）

番号	参照規則	提出資料	分類I		分類 II 及び III	
			参考	承認	参考	承認
1	**2.2.1-3.(2)**及び **3.4.3-2.**	品質計画書	-	-	-	○*
2	**2.2.1-3.(3)**及び **3.4.3-3.**	コンピュータシステムの分類の一覧	参考（分類に関係なく）○			
3	**2.2.1-3.(4)**及び **3.4.3-4.**	リスク評価報告書 （システムの分類を決定するためのもの）	参考（分類に関係なく）○*			
4	**2.2.1-3.(5)**及び **3.4.3-5.**	船舶のシステムアーキテクチャ	○*	-	○*	-
5	**2.2.1-3.(6)**及び **3.4.3-6.**	SAT の試験方案	-	-	-	○
6	**2.2.1-3.(6)**及び **3.4.3-6.**	SAT の試験報告書	-	-	○	-
7	**2.2.1-3.(7)**及び **3.4.3-7.**	SOST の試験方案	-	-	-	○
8	**2.2.1-3.(7)**及び **3.4.3-7.**	SOST の試験報告書	-	-	○	-
9	**2.2.1-3.(8)**及び **3.4.3-8.**	変更管理手順書	-	-	-	○*

（備考）

承認：承認用図面及び資料

参考：参考用図面及び資料

○：提出

○*：本会／本会検査員が必要と認める場合に提出

システムの分類については **3.3.1** を参照

表 X2.3　　供給者による提出資料の概要（4 章「船上のシステム及び機器のサイバーレジリエンス」関連）

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))	船舶資産インベントリに組み込まれること (5.4.2(1))	-	○(1), (2)
2	トポロジー図 (4.4.1(2))	システム統合者がセキュリティゾーン及びコンジットを設計可能とするもの (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） (4.4.3)	-	○(1)
4	セキュリティ機能試験要領書 (4.4.1(4))	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） (4.4.3)	-	○(1)
5	セキュリティ構成指針 (4.4.1(5))	ネットワーク及びセキュリティ構成設定 (表 X4.1 中 29)	○(1)	-
6	セキュア開発ライフサイクル (4.4.1(6))	セキュア開発ライフサイクルに関する要件 (4.5)	-	○(1)
7	保守・検証手順書 (4.4.1(7))	セキュリティ機能の検証 (表 X4.1 中 19)	○(1)	-
8	インシデント対応・復旧計画支援情報 (4.4.1(8))	監査可能なイベント (表 X4.1 中 13) あらかじめ決定した出力 (表 X4.1 中 20) システムのバックアップ (表 X4.1 中 26) システムの復旧及び再構成 (表 X4.1 中 27)	○(1)	-
9	変更管理手順書 (4.4.1(9))	変更管理のプロセス (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
○：提出
(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

表 X2.4　　統合者又は船主による提出資料の概要（5 章「船舶のサイバーレジリエンス」関連）

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	-	-	-
4	船舶資産インベントリ（2.2.3-3.(6)）	提出	保守	保守	保守	-	-	-
5	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（2.2.3-3.(7)）*	提出	保守	保守	保守	-	-	-
6	補完的対策の説明（2.2.3-3.(8)）*	提出	保守	保守	保守	-	-	-
7	船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)）	-	提出	実証	保守	-	-	実証
8	船舶サイバーセキュリティ・レジリエンス計画書（2.2.3-5.(7)） - 変更管理（5.4.2(1)(d)iv） - ソフトウェアアップデートの管理（5.4.2(1)(d)iv） - ファイアウォールの管理（5.4.3(1)(d)iv） - マルウェア対策の管理（5.4.3(3)(d)iv） - アクセス制御の管理（5.4.3(4)(d)iv） - 機密情報の管理（5.4.3(4)(d)iv） - 遠隔アクセスの管理（5.4.3(6)(d)iv） - 携帯用及び可搬式デバイスの管理（5.4.3(7)(d)iv） - セキュリティ異常の検知（5.4.4(1)(d)iv） - セキュリティ機能の検証（5.4.4(2)(d)iv） - インシデントへの対応計画（5.4.5(1)(d)iv） - 復旧計画（5.4.6(1)(d)iv）	-	-	-	保守	提出	実証	-

（備考）

*：該当する場合に限る。

提出：利害関係者は，5 章に規定する要件への適合の検証及び承認のために，本会に書類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書類を最新の状態に保たなければならない。アップデートされた文書及び変更管理の記録は，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，承認された書類に従って，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

表 X2.5　　5 章「船舶のサイバーレジリエンス」の各要件に関連する資料の概要

船舶資産インベントリ（**5.4.2(1)**）		
コンピュータシステムセキュリティの機能	製品セキュリティアップデートに関する文書の提供 独立コンポーネントセキュリティアップデートに関する文書の提供 セキュリティアップデートの提供	**4.5.3** **4.5.4** **4.5.5**
コンピュータシステムの書類	コンピュータシステム資産インベントリ 変更計画の管理	**4.4.1(1)** **4.4.1(9)**
船舶の設計書類	船舶資産インベントリ	**5.4.2(1)(d)i)**
船舶サイバーセキュリティ・レジリエンス計画書	変更の管理	**5.4.2(1)(d)iv)**
	ソフトウェアアップデートの管理	**5.4.2(1)(d)iv)**
セキュリティゾーン及びネットワークセグメンテーション（**5.4.3(1)**）		
コンピュータシステムセキュリティの機能	-	-
コンピュータシステムの書類	トポロジー図	**4.4.1(2)**
船舶の設計書類	ゾーン及びコンジット図 設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.3(1)(d)i)** **5.4.3(1)(d)i)** **5.4.3(1)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	ゾーンにある境界デバイスのセキュリティ管理（例えば，ファイアウォール）	**5.4.3(1)(d)iv)**
ネットワークを防御する防護策（**5.4.3(2)**）		
コンピュータシステムセキュリティの機能	サービス拒否（DoS）からの防御 あらかじめ決定した出力	**表 X4.1** 中 **24** **表 X4.1** 中 **20**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順	**4.4.1(3)** **4.4.1(4)**
船舶の設計書類	船舶サイバーレジリエンス試験要領書	**5.4.3(2)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	-	-
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（**5.4.3(3)**）		
コンピュータシステムセキュリティの機能	悪意のあるコードからの保護	**表 X4.1** 中 **18**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順	**4.4.1(3)** **4.4.1(4)**
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.3(3)(d)i)** **5.4.3(3)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	マルウェア対策の管理	**5.4.3(3)(d)iv)**
アクセス制御（**5.4.3(4)**）		
コンピュータシステムセキュリティの機能	人間のユーザーの識別及び認証 アカウントの管理 識別子の管理 認証コードの管理 権限付与の実施	**表 X4.1** 中 **1** **表 X4.1** 中 **2** **表 X4.1** 中 **3** **表 X4.1** 中 **4** **表 X4.1** 中 **8**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順	**4.4.1(3)** **4.4.1(4)**
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.3(4)(d)i)** **5.4.3(4)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計	機密情報の管理	**5.4.3(4)(d)iv)**

画書	論理的及び物理的アクセスの管理	**5.4.3(4)(d)iv)**
無線通信（**5.4.3(5)**）		
コンピュータシステムセキュリティの機能	無線アクセスの管理 無線の使用の管理	**表 X4.1** 中 **5** **表 X4.1** 中 **8**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順	**4.4.1(3)** **4.4.1(4)**
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.3(5)(d)i)** **5.4.3(5)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	-	-
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（**5.4.3(6)**）		
コンピュータシステムセキュリティの機能	多要素認証 ソフトウェアプロセス／デバイスの識別及び認証 失敗したログイン試行 システム使用通知 信頼できないネットワーク経由のアクセス アクセス要求の明示的な承認 リモートセッションの終了 暗号化による完全性の保護 入力の検証 セッションの完全性 セッション ID の無効化	**表 X4.2** 中 **31** **表 X4.2** 中 **33** **表 X4.2** 中 **32** **表 X4.2** 中 **33** **表 X4.2** 中 **34** **表 X4.2** 中 **35** **表 X4.2** 中 **37** **表 X4.2** 中 **38** **表 X4.2** 中 **39** **表 X4.2** 中 **40** **表 X4.2** 中 **41**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順	**4.4.1(3)** **4.4.1(4)**
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.3(6)(d)i)** **5.4.3(6)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	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	**5.4.3(6)(d)iv)**
携帯用及び可搬式デバイスの使用（**5.4.3(7)**）		
コンピュータシステムセキュリティの機能	可搬式及び携帯用デバイスの使用の管理	**表 X4.1** 中 **10**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順	**4.4.1(3)** **4.4.1(4)**
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.3(7)(d)i)** **5.4.3(7)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	可搬式及び携帯用デバイスの管理	**5.4.3(7)(d)iv)**
ネットワーク動作の監視（**5.4.4(1)**）		
コンピュータシステムセキュリティの機能	可搬式及び携帯用デバイスの使用の管理 監査可能なイベント サービス拒否（DoS）攻撃からの保護 警報の過剰な帯域幅使用	**表 X4.1** 中 **10** **表 X4.1** 中 **13** **表 X4.1** 中 **24** **3.7.2-1.**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順	**4.4.1(3)** **4.4.1(4)**
船舶の設計書類	船舶サイバーレジリエンス試験要領書	**5.4.4(1)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	インシデント対応計画書	**5.4.4(1)(d)iv)**

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（5.4.4(2)）		
コンピュータシステムセキュリティの機能	セキュリティ機能の検証	表 X4.1 中 19
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 維持及び検証の計画	4.4.1(3) 4.4.1(4) 4.4.1(7)
船舶の設計書類	船舶サイバーレジリエンス試験要領書	5.4.4(2)(d)iii)
船舶サイバーセキュリティ・レジリエンス計画書	セキュリティ機能の検証	5.4.4(2)(d)iv)
インシデント対応計画書（5.4.5(1)）		
コンピュータシステムセキュリティの機能	-	-
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 インシデント対応計画書及び復旧計画書を支援する情報	4.4.1(8)
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	5.4.5(1)(d)i) 5.4.5(1)(d)iii)
船舶サイバーセキュリティ・レジリエンス計画書	インシデント対応計画書	5.4.5(1)(d)iv)
機側，独立及び／又は手動の操作（5.4.5(2)）		
コンピュータシステムセキュリティの機能	-	-
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 インシデント対応計画書及び復旧計画書を支援する情報	4.4.1(3) 4.4.1(4) 4.4.1(8)
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	5.4.5(2)(d)i) 5.4.5(2)(d)iii)
船舶サイバーセキュリティ・レジリエンス計画書	インシデント対応計画書	5.4.5(2)(d)iv)
ネットワークの分離（5.4.5(3)）		
コンピュータシステムセキュリティの機能	-	-
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 インシデント対応計画書及び復旧計画書を支援する情報	4.4.1(3) 4.4.1(4) 4.4.1(8)
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	5.4.5(3)(d)i) 5.4.5(3)(d)iii)
船舶サイバーセキュリティ・レジリエンス計画書	インシデント対応計画書	5.4.5(3)(d)iv)
ミニマルリスクコンディションへのフォールバック（5.4.5(4)）		
コンピュータシステムセキュリティの機能	あらかじめ決定した出力	表 X4.1 中 20
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 インシデント対応計画書及び復旧計画書を支援する情報	4.4.1(3) 4.4.1(4) 4.4.1(8)
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	5.4.5(4)(d)i) 5.4.5(4)(d)iii)

船舶サイバーセキュリティ・レジリエンス計画書	インシデント対応計画書	**5.4.5(4)(d)iv)**
復旧計画書（**5.4.6(1)**）		
コンピュータシステムセキュリティの機能	-	-
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 インシデント対応計画書及び復旧計画書を支援する情報	**4.4.1(3)** **4.4.1(4)** **4.4.1(8)**
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.6(1)(d)i)** **5.4.6(1)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	復旧計画書	**5.4.6(1)(d)iv)**
バックアップ及び復元の機能（**5.4.6(2)**）		
コンピュータシステムセキュリティの機能	システムのバックアップ システムの復旧及び再構成	**表 X4.1** 中 **26** **表 X4.1** 中 **27**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 インシデント対応計画書及び復旧計画書を支援する情報	**4.4.1(3)** **4.4.1(4)** **4.4.1(8)**
船舶の設計書類	船舶サイバーレジリエンス試験要領書	**5.4.6(2)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	復旧計画書	**5.4.6(2)(d)iv)**
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（**5.4.6(3)**）		
コンピュータシステムセキュリティの機能	システムの復旧及び再構成	**表 X4.1** 中 **27**
コンピュータシステムの書類	セキュリティ機能仕様書 セキュリティ機能のための試験手順 インシデント対応計画書及び復旧計画書を支援する情報	**4.4.1(3)** **4.4.1(4)** **4.4.1(8)**
船舶の設計書類	設計の説明 船舶サイバーレジリエンス試験要領書	**5.4.6(3)(d)i)** **5.4.6(3)(d)iii)**
船舶サイバーセキュリティ・レジリエンス計画書	復旧計画書	**5.4.6(3)(d)iv)**
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（**5.5**）		
コンピュータシステムセキュリティの機能	-	-
コンピュータシステムの書類	-	-
船舶の設計書類	コンピュータシステムを除外するためのリスク評価	**5.5**
船舶サイバーセキュリティ・レジリエンス計画書	-	-

2.2 試験

2.2.1 3章「コンピュータシステム」における試験

-1. **3 章**の適用を受けるコンピュータシステムは，当該コンピュータシステムの分類ごとに**-2.**及び**-3.**の各項に規定する，本会による検証を受けなければならない。また，本会検査員による立会又は検証が要求されるものの概要を，**表 X2.6**に示す。

-2. システム供給者に関する確認項目

(1) 品質計画書及び品質マニュアル（**3.4.2-1.**参照）

(a) 分類 I：本要件を適用外とする。（以下，本章において，「N/A」という。）

(b) 分類 II 及び III：

i) 品質計画書及び品質マニュアルを提出して本会の承認を得なければならない。

ii) 品質計画書及び品質マニュアルは，FAT の際に，本会検査員により確認可能でなければならない。

(2) システム及びソフトウェアの識別（**3.4.2-2.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：システム及びそのソフトウェアコンポーネントを識別できる方法が適用されていることにつき，FAT（**3.4.2-7.**参照）及び SAT（**3.4.3-6.**参照）の一部として確認を受けなければならない。

(3) システムの仕様書及び設計書（**3.4.2-3.**参照）

(a) 分類 I：本会が必要と認める場合，参考としてシステムの仕様書及び設計書の提出を要求することがある。

(b) 分類 II 及び III：システムの仕様書及び設計書を提出して本会の承認を得なければならない。

(4) ハードウェアコンポーネントの環境への適合性（**3.4.2-4.**参照）

(a) 分類 I：環境試験を省略して差し支えない。ただし，本会が必要と認める場合（**3.3.2** 参照），参考として**船用材料・機器等の承認及び認定要領第 7 編 1 章**に規定する使用承認の証明書又は **D 編 18.7.1(1)**に規定する環境試験を満足することを証明する資料の提出を要求することがある。

(b) 分類 II 及び III：参考として，**船用材料・機器等の承認及び認定要領第 7 編 1 章**に規定する使用承認の証明書又は **D 編 18.7.1(1)**に規定する環境試験を満足することを証明する資料を提出しなければならない。

(5) ソフトウェアコードの作成，パラメタリゼーション及び関連する試験（**3.4.2-5.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：本会検査員が必要と認める場合，参考としてソフトウェアの試験報告書の提出を要求することがある。

(6) FAT 前にシステム供給者が行うシステム試験（**3.4.2-6.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：

i) FAT 前にシステム供給者が行うシステム試験の試験報告書は，FAT の際に，本会検査員により確認可能でなければならない。

ii) 本会検査員が必要と認める場合，参考として当該試験の試験報告書を要求することがある。

(7) 船舶に搭載する前の FAT（**3.4.2-7.**参照）

(a) 分類 I：N/A

(b) 分類II及びIII：

i) FAT の試験方案を，当該試験実施前に提出して本会の承認を得なければならない。

ii) FAT は本会検査員の立会の下で実施しなければならない。

iii) FAT の試験報告書は，参考として提出されなければならない。

iv) ユーザーマニュアル，**-6.**に規定する試験の報告書等の追加の関連資料は，FAT の際に，本会検査員により確認可能でなければならない。

v) 本会が必要と認める場合，参考としてユーザーマニュアル，**-6.**に規定する試験の報告書等の追加の関連資料を要求することがある。

(8) 船上における安全かつ管理されたソフトウェアのインストール（**3.4.2-8.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：変更管理手順書を提出して本会の承認を得なければならない。なお，当該手順書は，品質計

画書及び品質マニュアルに含めても差し支えない。

-3. 統合者に関する確認項目

(1) 統合者の指名（**3.5.1** 参照）

所有者は，システム供給者と連携してシステムの変更を実施する責任を負う統合者を指定した場合には，それを本会へ適時に報告しなければならない。

(2) 品質計画書（**3.4.3-2.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：

i) 品質計画書は，検査（SAT/SOST）の際に，本会検査員により確認可能でなければならない。

ii) 本会が必要と認める場合，品質計画書を提出して本会の承認を得なければならない。

(3) システムの分類の決定（**3.4.3-3.**参照）

船舶に搭載するコンピュータシステムの分類の一覧を，参考として本会に提出しなければならない。

(4) システムのリスク評価（**3.4.3-4.**参照）

本会が必要と認める場合，参考としてシステムの分類を決定するためのリスク評価報告書を要求することがある。

(5) 船舶のシステムアーキテクチャの明示（**3.4.3-5.**参照）

分類 I，II 及び III：本会が必要と認める場合，参考として船舶のシステムアーキテクチャの提出を要求することがある。

(6) 船上における SAT（**3.4.3-6.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：

i) SAT の試験方案を，当該試験実施前に提出して本会検査員の承認を得なければならない。

ii) SAT は本会検査員の立会の下で実施しなければならない。

iii) SAT の試験報告書は，参考として本会へ提出されなければならない。

(7) 船舶レベルの SOST（**3.4.3-7.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：

i) SOST の試験方案を，当該試験実施前に提出して本会検査員の承認を得なければならない。

ii) SOST は本会検査員の立会の下で実施しなければならない。

iii) SOST の試験報告書は，参考として本会へ提出されなければならない。

(8) 変更管理（**3.4.3-8.**参照）

(a) 分類 I：N/A

(b) 分類 II 及び III：本会が必要と認める場合，変更管理手順書を提出して本会の承認を得なければならない。

表 X2.6　　本会検査員による立会及び確認の概要

参照規則	実施内容	責任者	分類 I	分類 II 及び III
2.2.1-2.(7)及び **3.4.2-7.**	FAT 立会	システム供給者	-	○
2.2.1-3.(6)及び **3.4.3-6.**	SAT 立会	統合者	-	○
2.2.1-3.(7)及び **3.4.3-7.**	SOST 立会	統合者	-	○
3.6.12.	変更管理の確認	統合者	-	○

（備考）

○：本会検査員による立会又は確認

システムの分類については **3.3.1** を参照

2.2.2　　4 章「船上のシステム及び機器のサイバーレジリエンス」における試験

-1. **4 章**の適用を受けるコンピュータシステムは，**-2.**から**-5.**に規定する製造工場等における試験を受けなければならない。

-2. 一般的な検査項目

供給者は，設計，製造及び内部での試験が完了したことを証明しなければならない。また，納入されるシステムが，承認された文書によって正確に示されていることを証明しなければならない。これは，システムを検査し，コンポーネント及び配置／構成をコンピュータシステム資産インベントリ（**4.4.1(1)**）及びトポロジー図（**4.4.1(2)**）と比較することによって実施しなければならない。

-3. セキュリティ機能試験

供給者は，納入するシステムにおいて，要求されるセキュリティ機能を試験しなければならない。当該試験にあっては，承認された試験方案（**4.4.1(4)**）に従って実施され，検査員が立会い，合格を確認しなければならない。また，当該試験にあっては，すべての要件が満たされていることを合理的に検査員に示さなければならない。これは，同一のコンポーネントに対する試験は通常省略することを意味する。

-4. セキュリティ機能の正確な設定

供給者は，検査員に対して，システムのコンポーネントがセキュリティ構成指針（**4.4.1(5)**）に従って構成されていることを試験／実証しなければならない。当該実証は，セキュリティ機能の試験と同時に実施することができる。セキュリティの設定は，報告書として文書化されなければならない。（個船毎の構成指針の事例等）

-5. セキュア開発ライフサイクル

供給者は，**4.4.1(6)**の文書に従って，**4.5** に規定するセキュア開発ライフサイクルの要件に適合していることを実証しなければならない。

(1) 秘密鍵の管理策（*IEC* 62443-4-1/SM-8）

秘密鍵の管理策は，ユーザーがその信頼性を確認できるようにすることを目的として，電子署名されたソフトウェアをシステムが含む場合に適用される。供給者は，コード署名に使用される秘密鍵の生成，保管及び使用を不正アクセスから保護することを目的として，ポリシー，手順及び技術的管理策が行われていることを立証するマネジメントシステム文書を提示しなければならない。ポリシー及び手順にあっては，役割，責任及び作業プロセスを扱わなければならない。技術的管理策にあっては，秘密鍵の保管に関して，例えば，物理的なアクセス制限や，暗号化ハードウェア（ハードウェアセキュリティモジュール等）が含まれなければならない。

(2) セキュリティアップデートの文書（*IEC* 62443-4-1/SUM-2）

供給者は，セキュリティアップデートを確実にユーザーに知らせるためのプロセスが，組織内に確立されていることを証明するための，マネジメントシステム文書を提示しなければならない。ユーザーへの情報提供は，**4.5.3** に記載された項目を含まなければならない。

(3) 依存コンポーネントのセキュリティアップデート文書（*IEC* 62443-4-1/SUM-3）

供給者は，**4.5.4** で要求されるように，システム内の取得したソフトウェアのアップデート版（オペレーティングシステム又はファームウェアの新バージョン／パッチ）にシステムが対応しているかどうかをユーザーに確実に知らせるプロセスが，組織内に確立されていることを証明するための，マネジメントシステム文書を提示しなければならない。また，アップデートされた取得済みのソフトウェアを適用しないことによるリスクを，どのように管理するかについても言及しなければならない。

(4) セキュリティアップデートの配信（*IEC* 62443-4-1/SUM-4）

供給者は，**4.5.5** で要求されるように，システムセキュリティのアップデートをユーザーが利用可能となることを確保するプロセスが，組織内に確立されていることを証明し，ユーザーがアップデートされたソフトウェアの信頼性を確認する方法を記述したマネジメントシステム文書を提示しなければならない。

(5) 製品の多層防御（*IEC* 62443-4-1/SG-1）

供給者は，**4.5.6** で要求されるように，インストール，保守及び運用中に，コンピュータシステムのソフトウェアに対するセキュリティ上の脅威を軽減するための，多層防御による対策の戦略を文書化するプロセスが組織内に確立されていることを実証する，マネジメントシステム文書を提示しなければならない。脅威の例としては，許可されていないソフトウェアのインストール，パッチ適用プロセスの脆弱性，船舶の運用段階でのソフトウェアの改ざん等が考えられる。

(6) 環境において期待される多層防御による対策（*IEC* 62443-4-1/SG-2）

供給者は，**4.5.7** で要求されるように，物理的な配置，ポリシー，手順等の，外部環境によって提供されることが期待される多層防御による対策を文書化するプロセスが，組織内に確立されていることを実証するマネジメントシステム文書を提示しなければならない。

(7) セキュリティハードニング指針（*IEC* 62443-4-1/SG-3）

供給者は，**4.5.8** で要求されるように，システムに対して強化ガイドラインが作成されることを保証するプロセスが，組織内に確立されていることを実証するマネジメントシステム文書を提示しなければならない。当該ガイドラインは，不要なソフトウェア，アカウント，サービス等の削除／禁止／無効化によってシステムの脆弱性を低減する方法を指定しなければならない。

2.2.3 5章「船舶のサイバーレジリエンス」における試験

-1. **5章**の適用を受けるコンピュータシステムは，**-2.**から**-5.**に規定する適合の実証のための試験を受けなければならない。

-2. 一般

(1) **5章**に規定する要件への適合の評価は，以下に規定される各段階における関連する文書及び検査による評価が本会によって実施されなければならない。

(2) 供給者が本会に提出する文書は，**4章**に規定されている。この承認されたバージョンの文書は，**4.6.2** に規定するように，供給者から統合者にも提供されなければならない。

(3) 統合者が提供する文書は，**2.2.3-3.**及び**-4.**に記載されている。

(4) 船主が提供する文書は，**2.2.3-5.**に記載されている。

(5) 船舶の引渡し時に，統合者は，以下の文書を船主に提供しなければならない。

(a) 供給者が提供するコンピュータシステムの文書（**4.6.2**）

(b) 統合者が作成する文書（**2.2.3-3.**及び**-4.**参照）

-3. 設計及び建造段階

(1) 供給者は，**4.6** に規定された認証プロセスに従うことにより，本会に対して適合を実証しなければならない。

(2) 統合者は，評価のために本章に規定する文書を本会に提出することにより，適合を実証しなければならない。

(3) 設計及び建設段階において，設計の修正は，**3.6** に規定する変更管理の要件に従って実施しなければならない。

(4) ゾーン及びコンジット図については，**5.4.3(1)(d)i)**を参照すること。

(5) サイバーセキュリティデザインの説明（CSDD）については，**5.4** に規定する各要件の「適合の実証」中，「設計段階」の項目を参照すること。

(6) 船舶資産インベントリについては，**5.4.2(1)**を参照すること。

(7) 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については，**5.5** を参照すること。

(8) 本章の適用範囲内にあるいずれかのコンピュータシステムが，**4章**の代わりに補完的対策によって承認されている場合，当該文書は，それぞれのコンピュータシステム及び不足しているセキュリティ能力を明記し，補完的対策の詳細な説明を提供しなければならない。供給者がシステム文書にそのような補完的対策を記述することを要求する **4.4.1(3)**も参照すること。

-4. 船舶の運航時

(1) 船舶の最終的な試験の前に，統合者は以下を実施しなければならない。

(a) 最新の設計書類を本会に提出する（**2.2.3-3.**に規定する書類を実態にあわせて更新したもの）

(b) 試験及び／又は分析評価によって **5章**への適合を実証する方法を記述した船舶サイバーレジリエンス試験要領書を本会に提出する。

(c) 承認された船舶サイバーレジリエンス試験要領書に従って，本会の立会試験を実施する。

(2) 船舶サイバーレジリエンス試験要領書

(a) この文書の内容は，**5.4** に規定する各要件の「適合の実証」中，「試運転段階」の項目に規定されている。

(b) 各コンピュータシステムについて，要求される固有のセキュリティ機能及びその構成は，各コンピュータシステムの承認プロセスで検証及び試験される（**4章**参照）。このようなセキュリティ機能の試験は，**5.4** に規定する各要件中，「試運転段階」で明記されている場合は，これらのセキュリティ機能が **4章**によるコンピュータシステムの承認中に正常に試験されていることを条件として省略することができる。ただし，すべての試験は船舶サイバーレジリエンス試験要領書に含まれなければならず，試験を省略するか否かは本会が決定する。承認プロセスから試運転段階に気づき／コメントが引き継がれる場合，補完的対策によってそれぞれの要件が満たされている場合又は承認プロセス後のコンピュータシステムの変更等のその他の理由がある場合には，一般的に試験を省略してはならない。

(c) 船舶サイバーレジリエンス試験要領書では，**2.2.3-3.(8)**に記載されている補完的対策の試験方法も明らかにす

るものとする。

(d) 船舶サイバーレジリエンス試験要領書には，ステータスのアップデート手段及び試験中に結果を記録する手段を含め，以下の情報を明らかにしなければならない。

i) 必要とされる試験準備（すなわち，同様の予想される結果でテストを繰り返すことができることを保証すること。）

ii) 試験装置

iii) 初期条件

iv) 試験方法，詳細な試験手順

v) 予想される結果及び合格基準

(e) 船舶サイバーレジリエンス試験要領書を本会に提出する前に，統合者は，情報がアップデートされ，変更管理下に置かれていることを確認しなければならない。当該手順は，船上に搭載されているコンピュータシステム及びそれらと接続するネットワークの最新の構成と一致していること，船上に搭載されていない他のコンピュータシステム（例えば，陸上）及び船上に搭載されているコンピュータシステム及びネットワークの最終構成に関する関連要件を満たすため並びに採用された対策の実施の検証及び動作の検証を可能にするために，文書化された試験が十分に詳細であること。

(f) 統合者は，完全に統合された船舶におけるセキュリティ制御及び対策の検証テスト又は評価を文書化し，構成の変更管理を維持し，船舶サイバーレジリエンス試験要領書で対処された特定の状況又は障害によって安全な状態が影響を受ける可能性がある場合には，文書化された試験結果にそれらを記載しなければならない。

(g) 試験は，コンピュータシステムのための他の試運転が完了した後に，承認された船舶サイバーレジリエンス試験要領書に従って船上で実施しなければならない。本会は，追加のテストの実施を要請することがある。

-5. 船舶の運用期間中

(1) 船舶が船主に引き渡された後，船主は，**5 章**に規定されたプロセスを確立及び実施することにより，技術的及び組織的な安全対策を管理しなければならない。

(2) **5 章**の適用範囲内にあるコンピュータシステムの改造は，**3.6** に規定する変更管理に関する要件に従って実施されなければならない。当該要件には，コンピュータシステムの文書を最新の状態に保つことが含まれる。

(3) 船主は，供給者の支援を得て，船舶サイバーレジリエンス試験要領書を最新の状態に保ち，船舶に搭載されているコンピュータシステム，それらのシステムと相互に接続するネットワーク及び搭載されていない他のコンピュータシステム（例えば陸上）と整合させなければならない。船主は，船舶に搭載されているコンピュータシステム及びネットワークで発生した変更，そのような変更に関連する可能性のある新たなリスク，新たな脅威，新たな脆弱性並びに船舶の運用環境におけるその他の可能性のある変更を考慮して，船舶サイバーレジリエンス試験要領書をアップデートしなければならない。

(4) 船主は，船上のコンピュータシステム及び当該システムを相互に又は船舶外の他のコンピュータシステム（例えば陸上）に接続するネットワークに習熟させ，要件を満たすために採用された措置を適切に管理するために，操作手順の作成及び実施，定期的な訓練の提供並びに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。

(5) 船主は，供給者の支援を得て，例えば，船上のコンピュータシステム及び当該システムを接続するネットワークのハードウェア及びソフトウェアの定期的な保守により，要件を満たすために採用された措置を最新の状態に維持しなければならない。

(6) 船主は，試験の実施結果及び最新の船舶サイバーレジリエンス試験要領書の写しを船上に保管し，本会が利用できるようにしなければならない。

(7) 初回の年次検査

(a) 船主は，船舶の初回の年次検査の前の適切な時期に，**5 章**の適用範囲内にあるコンピュータシステムのサイバーセキュリティ及びサイバーレジリエンスの管理を文書化した船舶サイバーセキュリティ・レジリエンス計画書を本会に提出しなければならない。

(b) 船舶サイバーセキュリティ・レジリエンス計画書には，**5.4** に規定される各要件中，「適合の実証」に規定されたプロセス／活動を文書化したポリシー，手順，計画及び／又はその他の情報が含まれなければならない。

(c) 本会が船舶サイバーセキュリティ・レジリエンス計画書を承認した後，船主は，承認された船舶サイバーセキュリティ・レジリエンス計画書に記載されたプロセスの実施に関する記録又はその他の文書化された証拠を

提示することにより，初回の年次検査において適合を実証しなければならない。

(d) 船舶管理会社の変更は，船舶サイバーセキュリティ・レジリエンス計画書の新たな検証を必要とする。

(8) 2 回目以降の年次検査

その後の船舶の年次検査において，船主は，本会の要請に応じて，船舶サイバーセキュリティ・レジリエンス計画書の実施を実証しなければならない。

(9) 定期検査

船主は，船舶の船級証書がアップデートされた際に，船舶サイバーレジリエンス試験要領書に従って，本会の立会試験を実施しなければならない。一般に，安全保障措置は定期検査において実証されなければならないが，いくつかの安全保障措置は **5.4** に規定する各要件の「適合の実証」中，「運用段階」に規定されるコンピュータシステムの変更に基づいて，本会の要請があった場合に実施される。

3章　コンピュータシステム

3.1　一般

3.1.1　適用

本章の規定は，鋼船規則が適用されるコンピュータシステム並びにそれを構成するハードウェア及びソフトウェアの設計，構築，試験及び保守に適用する。ただし，国際条約に規定されるコンピュータシステム（例えば次の**(1)**から**(4)**に掲げるもの）には適用しない。

(1) **安全設備規則**に規定する航海設備
(2) **無線設備規則**に規定する無線設備
(3) 復原性計算機
(4) 積付計算機

3.1.2　参照規格

コンピュータシステムのハードウェア又はソフトウェアの開発に際して，以下に掲げる規格を参考にすることができる。また，これら以外の産業規格も考慮することができる。

(1) *IEC* 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems
(2) *ISO/IEC* 12207:2017 Systems and software engineering - Software life cycle processes
(3) *ISO* 9001:2015 Quality Management Systems – Requirements
(4) *ISO/IEC* 90003:2018 Software engineering - Guidelines for the application of ISO 9001:2015 to computer software
(5) *IEC* 60092-504:2016 Electrical installations in ships - Part 504: Special features - Control and instrumentation
(6) *ISO/IEC* 25000:2014 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Guide to SQuaRE
(7) *ISO/IEC* 25041:2012 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Evaluation guide for developers, acquirers and independent evaluators
(8) *IEC* 61511:2016 Functional safety - Safety instrumented systems for the process industry sector
(9) *ISO/IEC* 15288:2015 Systems and software engineering - System life cycle process
(10) *ISO* 90007:2017 Quality management - Guidelines for configuration management
(11) *ISO* 24060:2021 Ships and marine technology - Ship software logging system for operational technology

3.1.3　本章の構成

-1. **3.2** には，コンピュータシステムの承認の要件及び承認と使用承認との関係について規定する。

-2. **3.3** には，コンピュータシステムの分類について規定する。コンピュータシステムに関する要件及び確認の範囲は，当該分類に応じて決定される。

-3. **3.4** には，コンピュータシステムの開発及び納入について規定し，**3.5** には，運用段階における保守について規定する。なお，本章の要件は，コンピュータシステムの設計から運用までのライフサイクルにおける各段階ごとに，要件を満たすために必要な役割に分けて規定している。

-4. **3.6** には，本章において重視している，ソフトウェア及びシステムの変更管理の過程について規定する。

-5. **3.7** には，コンピュータシステムに関する技術要件について規定する。なお，同節を除く本章の要件は，主に，実行すべき作業の内容に焦点を当てて規定している。

-6. なお，各規定に関する提出図面等及び試験の要件については，**2章**に規定する。

3.1.4　用語

本章における用語の定義は，次の**(1)**から**(24)**による。

(1) 「ブラックボックスの記述」とは，当該システムの外部から確認される，システムの機能，動作及び性能に関する記述をいう。
(2) 「ブラックボックステスト」とは，入力の操作や出力の確認のみにより，システム，サブシステム及びコンポーネントの機能，性能及び堅牢性の確認を行う手法をいう。これは，システムの内部動作に関する知識を必要とせずに，テスト対象のシステムやコンポーネントの確認可能な動作のみに注目して，目的のレベルの確認を実現する。

(3) 「コンピュータシステム」とは，情報の収集，処理，保守，使用，共有，発信，処分等，1 つ以上の定められた目的を達成するために組織化されたプログラム可能な電子デバイス又は相互運用できる複数のプログラム可能な電子デバイスをいう。船上のコンピュータシステムには，情報技術(IT)及び運用技術(OT)のシステムが含まれる。また，コンピュータシステムは，ネットワークを介して接続されたサブシステムの組合せである場合もある。船上のコンピュータシステムは，直接又は公共の通信手段（インターネット等）を介して，陸上のコンピュータシステム，他船のコンピュータシステム及び／又は他の施設と接続されることもある。

(4) 「故障モードの記述」とは，システム内の故障がもたらす影響について記述した資料であって，次の**(a)**から**(c)**に掲げるものをいう。（システムがサポートする機器の故障ではない）

(a) 評価の対象となる故障の一覧

(b) 当該各故障に対するシステムの応答に関する記述

(c) 当該各故障の結果に対するコメント

(5) 「所有者」とは，建造段階においては，船舶を発注する組織又は個人をいい，就航後においては，船舶を所有又は管理する組織をいう。

(6) 「パラメタリゼーション」とは，パラメータを変更することにより，システム及びソフトウェアの機能を設定及び調整することをいう。これは，コンピュータプログラミングを必要とせず，通常は操作者や利用者ではなく，システム供給者又はサービス提供者によって行われる。

(7) 「プログラマブル装置」とは，ソフトウェアが搭載された物理的な構成要素をいう。

(8) 「堅牢性」とは，異常な入力や状態に対応する能力をいう。

(9) 「サービス提供者」とは，本会に雇用されていない個人又は会社であって，機器製造者，造船所，船舶の所有者又はその他の顧客の要望により，検査業務に関連して行動し，船舶又は移動式海洋構造物での，測定，試験又は安全システムや機器の保守等のサービスを行うものをいう。それらの結果は，検査員が船級又は条約に関する承認や業務に影響を与える決定を下す際に使用される。

(10) 「シミュレーション試験」とは，制御される機器，通信網及び回線の一部もしくはすべてをシミュレーションツールにより置き換えた状態で行う監視，制御又は安全システムの試験をいう。

(11) 「証明書」とは，本会により発行された適合書類であって，次の**(a)**から**(c)**を含むものをいう。

(a) 適用規則及び要件に適合していること。

(b) 承認されたコンポーネントの完成品又は，コンポーネントの製造段階から採取されたサンプル（該当する場合）に対して，試験及び検査が実施されたこと。

(c) 本会検査員の立会いの下で又は事業所承認規則に従って，試験及び検査が実施されたこと。

(12) 「ソフトウェアコンポーネント」とは，ソフトウェアコードの一部分であって，当該コードに密接に関連した特定の機能を独立して提供するものをいう。

(13) 「ソフトウェアのマスターファイル」とは，ソフトウェアの元のソースを構成するファイルをいう。カスタムメイドのソフトウェアでは，これは読み取り可能なソースコードのファイルである場合があり，商用オフザシェルフ（COTS）ソフトウェアでは，バイナリファイルの形式が異なることがある。

(14) 「ソフトウェア構造」とは，異なるソフトウェアコンポーネントがどのように相互作用するかの概要をいい，一般にソフトウェアアーキテクチャ又はソフトウェアの階層構造と呼ばれる。

(15) 「サブシステム」とは，システムを構成する特定可能な一部分であって，特定の機能を有するものをいう。

(16) 「供給者」とは，サービス，システムのコンポーネント又はソフトウェアの供給を実施する個人又は組織の総称をいう。

(17) 「システム」とは，目的，機能及び性能が定義されたコンポーネント，機器及びロジックの組合せをいう。本章において，システムは，単一のシステム供給者から提供されるものとする。また，システム階層の例を**図 X3.1** に示す。

(18) 「システム・オブ・システムズ」とは，複数のシステムから構成されたシステムをいう。システム・オブ・システムズは，船舶の一部として造船所から供給されるすべての監視，制御及び安全システムを含む。

(19) 「システム供給者」とは，統合者の調整のもとで，システムのコンポーネント又はソフトウェアの供給を実施する個人又は組織をいう。

(20) 「統合者」とは，コンピュータシステムのライフサイクルのすべての段階において，システム及びサブシステムの供給者間の調整を行う単一の組織又は個人をいう。当該調整の目的は，これらを承認された船舶全体のシステム・

オブ・システムズへ統合し，コンピュータシステムの適切な運用及び保守を行うことである。特に指定されない場合には，設計から引渡しまでは造船所，運用段階では所有者を統合者とする。

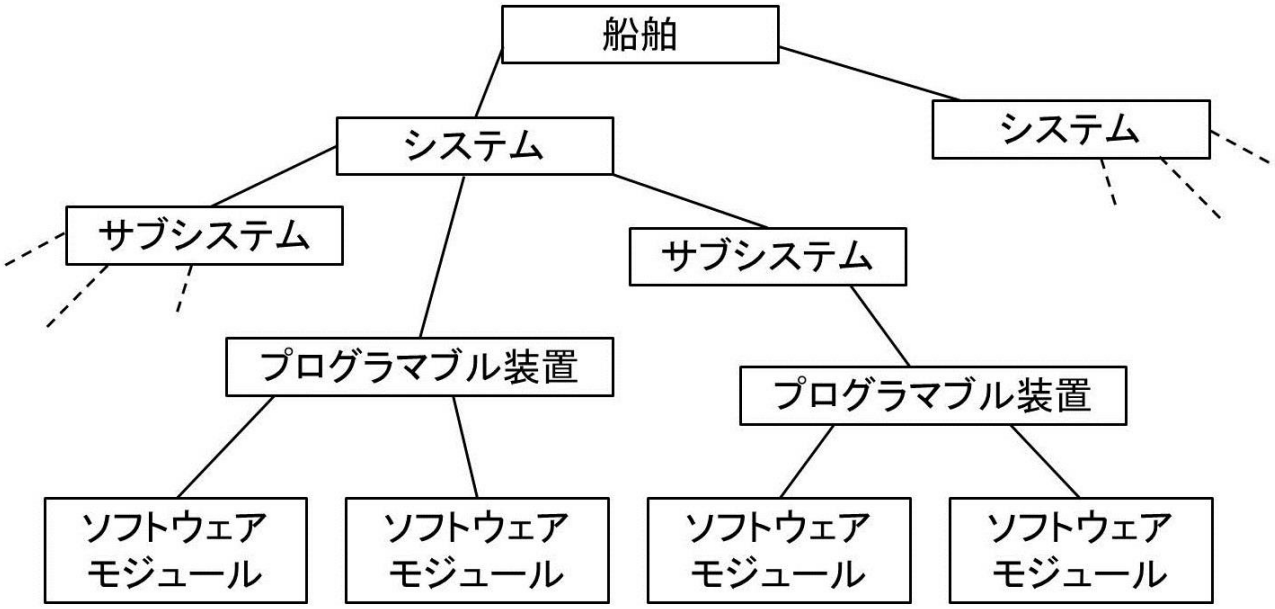
(21) 「船舶」とは，コンピュータシステムが搭載される船舶（海洋構造物を含む）をいう。

(22) 「FAT」とは，**3.4.2-7.**に規定する船舶に搭載する前の製造工場等における試験をいう。

(23) 「SAT」とは，**3.4.3-6.**に規定する船上におけるシステム検証試験をいう。

(24) 「SOST」とは，**3.4.3-7.**に規定する船上における最終的な環境でのシステム・オブ・システムズ（SoS）試験をいう。

図 X3.1　　システム階層の例



3.2　システム及びコンポーネントの承認

3.2.1　システムの承認*

-1.　分類Ⅱ又は分類Ⅲ（**3.3.1** にて定義するもの）に該当する，船舶の機能を達成するために必要なコンピュータシステムは，船舶向けの証明書と共に納入されなければならない。船舶向けにシステムを承認する目的は，システムの設計及び製造が完了し，当該システムが関連要件に適合していることを確認することである。船舶向けのシステムの承認を受けるための試験等は，主に次の**(1)**及び**(2)**によって構成される。

(1)　船舶向けのシステムに関する資料の評価（**3.4.2** 及び **3.6** 参照）

(2)　船舶に搭載されるシステムに関する検査及び試験（**3.4.2-7.**参照）

-2.　前**-1.**に規定する要件に適合していることの確認及び船舶向けの証明書の発行に際しては，本会が別に定めるところにより，**事業所承認規則**を適用することができる。

3.2.2　コンピュータシステムの使用承認

-1.　標準化されたソフトウェアを搭載し，継続的に製造されるコンピュータシステムは，**船用材料・機器等の承認及び認定要領 第 7 編 8 章**に従って使用承認を受けることができる。**3.4.2-4.**に規定するハードウェアの環境試験に関する書類については，**2.2.1-2.(4)**による。使用承認を受けるための試験等は，主に次の**(1)**及び**(2)**によって構成される。

(1)　使用承認の対象となるシステムに関する資料の評価

(2)　標準化された機能についての検査及び試験

-2.　使用承認を受けたコンピュータシステムであっても，原則として，**3.2.1** に規定する船舶向けのシステムの承認が必要となる。ただし，当該コンピュータシステムに関して，提出図面等については **2.1.1(1)(a)**及び**(2)(a)**のただし書きによることができ，また，試験については **3.2.1-2.**によることができる。

3.3 システムの分類

3.3.1 システムの分類の定義

システムは，その故障が人体及び船体並びに環境に及ぼしうる影響の度合いに応じ，**表 X3.1** のとおり分類 I，分類 II 又は分類 III に分類される。

表 X3.1 コンピュータシステムの分類

分類	故障時の影響度合い	システムの典型的な機能
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	- 監視，情報及び管理業務に関する機能
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	- 船舶の正常な運航及び居住状態を維持するために必要な警報，監視及び制御機能
III	故障が人体及び船体への危険又は壊滅的状態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	- 船舶の推進及び操舵を維持するための制御機能 - 船舶の安全に関する機能

3.3.2 適用範囲

分類 I のシステムは，その故障が危険な状況に帰結しないため，原則として，本会による確認の対象とはならない。しかし，適切な分類を決定するため又は分類 II 及び III のシステムの動作に影響を与えないことを確認するため，本会が必要と認める場合には，分類 I のシステムに関連する情報を要求することがある。

3.3.3 システムの分類の例*

システムの分類は，常に対象船舶ごとに評価されなければならない。このため，システムの分類は船舶によって異なる場合もあるが，分類の例（網羅的なものではない）を以下に示す。なお，各船舶に対するシステムの分類の決定については，**3.4.3-3.**によらなければならない。

(1) 分類 I のシステムの例
  (a) 燃料監視システム
  (b) 保守支援システム
  (c) 診断及びトラブルシューティングシステム
  (d) CCTV
  (e) 居室のセキュリティ
  (f) 娯楽設備
  (g) 魚群探知器

(2) 分類 II のシステムの例
  (a) 燃料制御システム
  (b) 主機及び補機の警報システム
  (c) イナートガス装置
  (d) 貨物格納設備の制御，監視及び安全システム

(3) 分類 III のシステムの例
  (a) 主機の制御装置
  (b) 操舵装置の制御システム
  (c) 電源装置（パワーマネジメントシステムを含む）
  (d) 2 級及び 3 級自動船位保持設備

3.4 コンピュータシステムの開発及び承認に関する要件

3.4.1 一般

-1. 適切な規格によるライフサイクルアプローチ

ハードウェア及びソフトウェアの設計及び開発並びにサブシステム，システム及びシステム・オブ・システムズの統合は，システムのライフサイクルにわたり，包括的なトップダウン方式であって，本章に掲げる規格又はその他の本会が適

当と認める規格に基づくものにより実施されなければならない。このことは，**-2.**に示す品質管理システムの検証の一部として，本会により確認される。

-2. 品質管理システム

統合者及びシステム供給者は，分類 II 及び III のコンピュータシステムの品質管理において，*IEC/ISO* 90003 にいう原則も考慮し，*ISO* 9001 等の品質管理システムに関する規格に準拠しなければならない。品質管理システムは，分類 II 及び III のコンピュータシステムに関して，少なくとも**表 X3.2** に掲げる項目を含むものでなければならない。また，本会による品質管理システムの検証は，次の**(1)**又は**(2)**のいずれかによることができる。

(1) 品質管理システムが，該当する規格に適合している旨，既に認証されていることの確認。なお，当該認証は，いずれかの国の認定制度に基づいて認定された認証機関が行ったものであること。

(2) 品質管理システムを本会が評価して行う，該当する規格に適合している旨の確認。なお，各資料に関する要件については，個別に決定する。

表 X3.2　　品質管理システムの内容

範囲		役割	
番号	内容	システム供給者	統合者
1	従業員の責任及び適格性	○	○
2	納入されるソフトウェア及び関連するハードウェアのライフサイクル全般	○	○
3	コンピュータシステム並びにそのコンポーネント及びバージョンを識別するための具体的な手順	○	-
4	船舶のシステムアーキテクチャの作成及び更新	-	○
5	ソフトウェア及び関連するハードウェアを供給者から取得するための担当部署又は組織等	○	○
6	ソフトウェアコードを作成及び確認するための担当部署又は組織等	○	-
7	船上において統合する前にシステムを検証するための担当部署又は組織等	○	-
8	FAT 又は SAT における実施及び承認の具体的な手順	○	○
9	文書の作成及び更新	○	-
10	造船所及び所有者との連絡を含む，ソフトウェアの変更及び船上におけるインストールの具体的な手順	○	○
11	ソフトウェアコードを確認する具体的な手順	○	-
12	システムと他のシステムとの統合手順及びシステム・オブ・システムズの試験手順	○	○
13	FAT 前における，ソフトウェア及び構成の変更を管理するための手順	○	-
14	FAT 後における，ソフトウェア及び構成の変更を管理及び記録するための手順	○	○
15	品質管理システムの遵守を組織自身が確実にするための確認項目	○	○

（備考）

○：品質管理システムに含めなければならない。

3.4.2　　システム供給者に関する要件*

-1. 品質計画書及び品質マニュアル

(1) システム供給者は，対象システムの設計，製造，納入及び保守に品質管理システムが適用される旨を品質計画書及

び品質マニュアルに記載しなければならない。

(2) **表 X3.2** において，システム供給者に適用されるすべての項目が含まれ，かつ，遵守されていることを示さなければならない。

-2. システム及びソフトウェアの識別

システム及びそのソフトウェアコンポーネント（バージョン情報を含む）を一意的に識別できる方法が，当該システム及びソフトウェアのライフサイクルにわたって適用されなければならない。当該システムに関する技術要件については，**3.7.1** による。識別方法の記載は，通常，**3.4.1-2.**に規定する品質管理システムの一部に含まれる。

-3. システムの仕様書及び設計書

(1) システムの仕様及び設計を決定し，システムの仕様書及び設計書に記載しなければならない。システムの仕様書及び設計書は，詳細な設計や実装の仕様書として機能するだけでなく，システム全体が仕様に従って，適用される規則や規制を遵守していることを文書化することを目的とする。

(2) システムの仕様書及び設計書は，次の**(a)**から**(h)**を含むものでなければならない。

(a) 目的及び主な機能（安全面を含む）

(b) システムの分類

(c) 主要な性能特性

(d) 適合する技術要件及び船級規則

(e) ユーザーインターフェース／ミミック

(f) コミュニケーション及びインターフェース
船内の他のシステムとのインターフェースの識別及び説明

(g) 関連するハードウェアの配置

i) ネットワーク・アーキテクチャ/トポロジー（スイッチ，ルーター，ゲートウェイ，ファイアウォール等のすべてのネットワークコンポーネントを含む）

ii) システム内のすべてのインターフェース及びハードウェアノードに関する内部構造（例：操作場所，表示器，コンピュータ，プログラム可能なデバイス，センサー，アクチュエーター，I/O モジュール等）

iii) I/O 割付（フィールド機器とチャネル，通信リンク，ハードウェアユニット及びロジックファンクションとのマッピング）

iv) 電源システムの構成

(h) FMEA（故障モード影響解析）によるリスク評価報告書又は当該リスク評価を省略することの妥当性を示す資料

-4. ハードウェアコンポーネントの環境への適合性

システム及びサブシステムを含む，ハードウェアの環境試験については，**D 編 18.7.1(1)**を満足しなければならない。

-5. ソフトウェアコードの作成，パラメタリゼーション及び関連する試験

(1) プロジェクトに応じて作成，変更又は構成されるソフトウェアは，品質計画書及び品質マニュアルに定めた規格に従って，開発され，品質保証活動が評価されなければならない。

(2) 品質保証活動は，ソフトウェア構造における様々なレベルで実施することができ，必要に応じて，カスタムメイドのソフトウェアと設定したコンポーネント（ソフトウェアライブラリ等）の両方を含まなければならない。

(3) ソフトウェアの検証は，ブラックボックステストの手法に基づき，少なくとも，次の**(a)**から**(c)**について確認しなければならない。

(a) ソフトウェアコンポーネントにおけるパラメタリゼーション及び構成の正確性，完全性及び一貫性

(b) 意図する機能

(c) 意図する堅牢性

(4) 分類 II 及び III のシステム内のコンポーネントについては，実施したすべての評価，分析，試験及びその他の検証活動の範囲，目的及び結果を試験報告書に記載しなければならない。

-6. FAT 前にシステム供給者が行うシステム試験

(1) FAT の前に，できる限りシステム試験を行わなければならない。システム試験の主たる目的は，システムが全体にわたり，仕様書，承認資料，適用される規則及び規定に適合していること，また，システムが完成し，FAT の準備が整っていることを，システム供給者が確認することである。

(2) 本試験では，少なくとも，システムに関して次の**(a)**から**(f)**に掲げる事項を確認しなければならない。

(a) 機能性
(b) 故障及び不具合の影響（診断機能，検知，アラートに対する応答を含む）
(c) 性能
(d) ソフトウェア及びハードウェアのコンポーネント間の統合
(e) ヒューマンマシンインターフェース
(f) 他のシステムとのインターフェース

(3) システムの適切な障害検知及びその際の応答を実証するため，可能な限り実際の使用状況に沿った障害を模擬しなければならない。
(4) 試験の一部は，シミュレータ及び当該ハードウェアを模擬したものを使用して実施することができる。
(5) 試験環境については，シミュレータ，エミュレータ，テストスタブ，試験管理ツール又は試験環境に影響を与えるその他のツールについての説明及びその制限を含めて，文書化されなければならない。
(6) テストケース及び試験結果は，それぞれ試験方案及び試験報告書に文書化されなければならない。

-7. 船舶に搭載する前の FAT

(1) FAT は，個品ごとに又は**船用材料・機器等の承認及び認定要領第 7 編 8 章**に従いコンピュータシステムの使用承認を取得する際に実施しなければならない。本試験の主たる目的は，システム完成後，適用される規則に適合していることを本会により確認することである。試験の結果が適当と認められた場合，本会により，当該システムに対して個船向けの証明書が発行される。
(2) FAT 試験方案は，システム供給者が行うシステム試験（**3.4.2-6.**参照）から代表的な試験項目を選択し，通常のシステムの機能及び障害に対する応答を含むものとする。
(3) 分類Ⅱ及びⅢのコンピュータシステムについては，**3.7.2-1.**に規定するネットワークレジリエンスの要件への適合を確認するため，ネットワーク試験を実施しなければならない。ただし，関係者全員が同意した場合には，ネットワーク試験は，本船上における SAT の一部として行うことができる。
(4) FAT は，機能及び故障時の応答のシミュレーションに必要な手段も用いて，原則として，船上に設置される実際のハードウェアコンポーネントで動作する，プロジェクトに応じたソフトウェアで実施しなければならない。ただし，本会が適当と認める場合には，模擬のハードウェア，エミュレータ等の他の手段を使用することができる。
(5) 試験報告書には，各試験項目の合否を記載し，試験結果を記録しなければならない。また，試験報告書には，試験時にシステムにインストールされていたソフトウェア（ソフトウェアバージョンを含む）の一覧を記載しなければならない。

-8. 船上における安全かつ管理されたソフトウェアのインストール

(1) システムにおけるソフトウェアコンポーネントの初期インストール及びその後の変更は，システム供給者及び統合者の間で合意された変更管理手順に従って行われなければならない。
(2) 変更管理手順は，**3.6** の要件に適合するものでなければならない。
(3) サイバーセキュリティに関する対策は，本会が適当と認めるところによる。

3.4.3 統合者に関する要件*

-1. 責任

造船所以外の組織又は個人が特に指定されている場合を除き，船舶の建造中は，造船所を統合者とする。

-2. 品質計画書

(1) 統合者は船舶に搭載されるシステムの搭載，統合，完成及び保守に品質管理システムが適用される旨を文書化しなければならない。
(2) **表 X3.2** において統合者に適用されるすべての項目が含まれ，かつ，遵守されていることを示さなければならない。

-3. システムの分類の決定

(1) 船舶に搭載される各システムについて，**3.3** に定義する故障の影響度合いに応じて，そのシステムがどの分類に該当するかを決定しなければならない。
(2) システムの分類については，該当するシステム供給者に伝えられなければならない。
(3) 本会は適切な分類を確認するために，リスク評価を要求することがある。

-4. システムのリスク評価

(1) 本会が必要と認める場合，システムに適用される分類を決定するために，該当する船舶における当該システムのリスク評価を実施し，システムの分類を決定するためのリスク評価報告書として文書化しなければならない。

(2) リスク評価の方法は本会が合意したものでなければならない。

-5. 船舶のシステムアーキテクチャの明示

(1) システム・オブ・システムズを規定し，文書化しなければならない。このアーキテクチャの記載は，個々のシステムに機能を割り当て，また，各システム間の主要なインターフェースを識別することにより，種々の組み合わされたシステムの分類決定及び開発のための基礎となるものである。

(2) システムアーキテクチャは，船舶レベルの SOST の基礎となるものでなければならない（**3.4.3-7.**参照）。

(3) システムアーキテクチャは，少なくとも次の**(a)**から**(d)**を含むものでなければならない。

(a) システムアーキテクチャ（システム・オブ・システムズ）全体の概要

(b) 個々のシステムの目的及び主な機能

(c) 各システム間の通信及びインターフェース

(d) システム・オブ・システムズに対するリスク評価報告書

-6. 船上における SAT

(1) SAT は，本船上で実施しなければならない。SAT の主たる目的は，システムを搭載後，該当する船上の機械／電気／プロセスシステムとの統合後に，システムの機能（他の制御及び監視システムとのインターフェースのうち，可能なものを含む）を確認することである。

(2) 試験報告書には，各試験項目の合否を記載し，試験結果を記録しなければならない。また，試験報告書には，試験時にシステムにインストールされていたソフトウェア（ソフトウェアバージョンを含む）の一覧を記載しなければならない。

-7. 船舶レベルの SOST

(1) SOST は，各システムを搭載及び統合した後の，船上における最終的な環境で実施しなければならない。本試験の目的は，システム・オブ・システムズ全体の機能（すべてのインターフェース及び相互依存性を含む）が，要件及び仕様に適合していることを確認することである。

(2) SOST では，少なくとも，システム・オブ・システムズに関して次の**(a)**から**(e)**に掲げる事項を確認しなければならない。

(a) 相互に作用するシステム全体の機能性

(b) 故障時におけるシステム間の反応

(c) 性能

(d) ヒューマンマシンインターフェース

(e) 各システム間のインターフェース

-8. 変更管理

統合者は **3.6** に記載されるシステムの変更管理手順に従わなければならない。

3.5 コンピュータシステムの保守に関する要件

3.5.1 船舶の所有者に関する要件

船舶の所有者以外の組織又は個人が特に指定されている場合を除き，船舶の就航後は，船舶の所有者を統合者とする。また，システム供給者と連携してシステムへの変更について責任を有する統合者が指定された場合には，本会へ適時に報告されなければならない。

3.5.2 統合者に関する要件

変更管理については，次によらなければならない。また，分類 II 及び III のコンピュータシステムに関しては，**3.6.12** に規定する確認が，**B 編 3 章**に基づいて年次検査等の際に要求されることに留意すること。

(1) 統合者は，ソフトウェア及びハードウェアの変更管理に必要な手順書が船上に保持され，かつ，すべてのソフトウェアの変更及び更新を当該手順書に従って実施されることを確実にすること。変更管理の詳細については，**3.6** を参照すること。

(2) 運用中のコンピュータシステムに対する変更を記録すること。当該記録には，関連するソフトウェアのバージョン等，**3.6.11** に規定する内容を含めること。

3.5.3 システム供給者に関する要件

-1. 変更管理について，システム供給者は，**3.6** に規定する変更管理の手順を含む，システム保守の手順に従わなけれ

ばならない。

-2. 船上におけるシステムの変更に先立ち，システム供給者は，当該変更が，関連する社内試験に合格していることを確実にしなければならない。

-3. 分類 II 及び III のコンピュータシステムに関しては，3.6.12 に規定する確認が，B 編 3 章に基づいて年次検査等の際に要求されることに留意すること。

3.6 変更管理

3.6.1 一般

本 3.6 には，コンピュータシステムのライフサイクルにわたる変更管理について規定する。システムのライフサイクルにおける各段階において，通常は，関与するステークホルダーが異なるため，それに応じた変更管理手順を定めることができる。本会による確認内容については，3.6.12 に記載する。

3.6.2 変更管理手順の文書化

該当する組織は，対象となるコンピュータシステムのハードウェア及びソフトウェアの両方に適用される変更管理手順を定め，文書化しなければならない。FAT 後，システム供給者は，システムに対するすべての変更を，当該手順に従って管理しなければならない。例としては，ソフトウェアの新しいバージョン，新しいハードウェア，制御ロジックの変更，設定可能なパラメータの変更等の確認が挙げられる。手順書には，少なくとも 3.6.3 から 3.6.11 に規定する内容を記載しなければならない。3.6.8 に規定する影響度分析の結果によって，3.6.3 から 3.6.12 の要件をどの程度まで実施するかが決定される。ただし，3.6.11 に規定する変更記録は，常に作成しなければならない。

3.6.3 ステークホルダー間の合意*

変更管理のプロセスは，コンピュータシステムのライフサイクルの段階ごとに，関係するステークホルダー間で調整され，合意されなければならない。

3.6.4 承認されたソフトウェアの変更管理

該当するステークホルダー（通常は，FAT を実施した統合者及び本会）により承認された後に，システムに変更を加える場合には，変更管理手順書に従って実施されなければならない。

3.6.5 システム及びソフトウェアのバージョンの識別

システム供給者は，各システム及びソフトウェアのバージョンを一意的に識別できることを確実にしなければならない（3.4.2-2.参照）。

3.6.6 ソフトウェアのマスターファイルの取扱い

ソフトウェアコンポーネントのマスターファイルを構成するファイルの取扱いのための方法が定められなければならない。マスターファイルの完全性を確実にするために使用するツールや方法とともに，担当者の権限が明確に定められなければならない。

3.6.7 搭載されたソフトウェアのバックアップ及び復旧

船舶に搭載されたコンピュータシステムのソフトウェアコンポーネントのバックアップ及び復旧の方法が明確に定められなければならない。

3.6.8 変更前に行う影響度分析

システムに変更を加える前に，次の**(1)**から**(5)**を決定するための影響度分析を実施しなければならない。

(1) 変更の重要度

(2) 既存の資料への影響

(3) 必要な確認及び試験

(4) 変更について他のステークホルダーへ通知する必要性

(5) 変更前に他のステークホルダー（例えば本会又は所有者等）から承認を得る必要性

3.6.9 ソフトウェアの変更に失敗した場合のロールバック

システムの保守に，新しいバージョンのソフトウェアのインストールが含まれる場合，システムを以前の安定した状態に戻すことを目的として，当該インストールを行う前のバージョンのソフトウェアへのロールバックが実行可能でなければならない。ロールバックは，根本原因を明らかにして排除するために，文書化及び分析されなければならない。

3.6.10 システム変更の確認及び検証

現実的に最大限実行可能な限り，システムの変更は船上に搭載される前に確認されなければならない。搭載後，次の**(1)**

及び**(2)**を含む，文章化された検証方案に従い，船上にて確認されなければならない。

(1) 新機能及び／又は改良が想定した効果をもたらしていることの確認

(2) 変更が機能又は能力に想定外の悪影響を及ぼさないことを確認するための回帰テスト

3.6.11 変更記録

-1. システム及びソフトウェアの変更は，変更の可視化及びトレーサビリティを確実にするために，変更記録に記録されなければならない。変更記録には，少なくとも次の**(1)**から**(5)**を含むものでなければならない。

(1) 変更の目的

(2) 変更点及び修正点の説明

(3) 影響度分析の主な結論（**3.6.8** 参照）

(4) すべての新しいシステム又はソフトウェアバージョンの識別（**3.6.5** 参照）

(5) 試験結果又は試験概要（**3.6.10** 参照）

-2. ソフトウェアの変更に関する文書は，計画保全に用いるシステム，ソフトウェアレジストリ又は同等のものに記録しても差し支えない。

3.6.12 本会による変更管理の確認

-1. 就航後

就航後の変更管理に関する本会による確認は，通常，年次検査等の際に行う。変更管理手順書及び関連する変更記録（**3.6.11** 参照）は，当該検査の際に確認可能でなければならない。事前に本会による承認を必要とする変更の場合は，その際に当該変更の関連手順及び文書を確認することがある。

-2. 建造中

建造中の変更管理に関する本会による確認は，品質管理システムの検証の一部としての手順の確認（**3.4.1-2.**参照）並びに FAT 時（**3.4.2-7.**参照）及び FAT 後（**3.6.12-1.**参照）のプロジェクトに応じた手順実施の確認の 2 つに分けられる。

3.7 コンピュータシステムに関する技術要件

本 **3.7** には，コンピュータシステムに関する技術要件について規定する。当該要件への適合は，設計資料（**3.4.2-3.**参照）に文書化され，**2 章**に規定する確認を受けなければならない。

3.7.1 システム及びソフトウェアの識別及びバージョンの報告

システムは，その名称，バージョン，識別子及び製造者を識別する手段を有するものでなければならない。また，*ISO* 24060 に規定される Ship software logging system (SSLS)に，そのソフトウェアの状態を自動的に報告できるものであることを推奨する。

3.7.2 データリンク

-1. 分類Ⅱ及びⅢのシステムにおけるデータリンクに関する一般要件

データリンクは，次の**(1)**から**(5)**によらなければならない。また，データリンクの喪失は，リスク評価（FMEA）において特に検討されなければならない。（**3.4.2-3.**参照）

(1) データリンクにおける単一故障が，分類 III の船舶機能の喪失を引き起こすものでないこと。当該故障の影響は，船舶機能におけるフェールセーフの原則を満たすものであること。

(2) 分類 II 及び III の船舶機能について，遠隔制御システムの機能喪失は，機側／手動による手段で補えること。

(3) データリンクは，過度の通信速度について防止又は対処する手段を有するものであること。

(4) データリンクは，当該データリンクの故障及び性能上の問題並びにデータリンクに接続されたノードのデータ通信の故障を検出するための，自己診断機能を有するものであること。

(5) 故障が検出された際に警報を発するものであること。

-2. ワイヤレスデータリンクに関する特別要件

(1) 分類 III のシステムには，本会が認める国際規格又は国家規格に従って実施した工学的解析に基づいて本会の承認を得た場合を除き，ワイヤレスデータリンクを使用してはならない。

(2) その他の分類のシステムは，次の**(a)**から**(d)**に従うことを条件に，ワイヤレスデータリンクを使用することができる。

(a) 次の **i)**から **iv)**を含む国際的なワイヤレス通信規約に適合すること。

i) メッセージの完全性

受信メッセージに欠落及び改変が起こらないよう，障害の防止，検出，診断及び訂正による対策を講じること。

ii) 設定及び装置の承認
許可された装置の接続のみを可能とする設計であること。

iii) メッセージの暗号化
データが含む内容の機密性及び重要性を保護すること。

iv) セキュリティマネジメント
ネットワークの構成要素を保護するとともに，権限の無いアクセスを防止すること。

(b) 船上のシステム間の通信に使用されるワイヤレスデータリンクは，周波数及び電力レベルに関し，国際電気通信連合（ITU）の定める要件及び船籍国の法規等に適合すること。

(c) 無線周波数伝送の使用に関連する港湾国及び地域の規制が，周波数及び電力レベルの制限により無線データ通信リンクの運用を禁止する場合のシステム運用を考慮すること。

(d) 係留運転及び海上試運転により，想定される動作環境においてワイヤレスデータリンクに関連する通信機器が次の **i)**及び **ii)**に掲げる事項を満足することを確認すること。

i) 当該機器の無線通信による電磁的干渉が他のいかなる機器の障害を引き起こさないこと。

ii) 電磁的干渉により当該機器に障害が発生しないこと。

3.7.3 本会による技術要件の検証

本 **3.7** に規定する技術要件に関する本会による確認は，システムの仕様書及び設計書（**3.4.2-3.**参照）の確認，FAT（**3.4.2-7.**参照）及び SAT（**3.4.3-6.**参照）の一部として行う。

4章　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

4.1.1　通則*

本章は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要件を規定するものである。

4.1.2　適用

-1. 本章の適用は，次の**(1)**及び**(2)**による。

(1) 本章の規定は，次に掲げる船舶に適用する。
  (a) 国際航海に従事する旅客船（旅客船に該当する高速船を含む）
  (b) 国際航海に従事する総トン数 500 トン以上の貨物船
  (c) 国際航海に従事する総トン数 500 トン以上の高速船
  (d) 総トン数 500 トン以上の海底資源掘削船
  (e) 建設に従事する自航式海洋構造物（すなわち，風力発電設備の設置，保守及び補修，クレーンユニット，ドリリングテンダー，宿泊等に用いられるもの）

(2) 本章の規定は，次に掲げるものに対して，非強制の指針として用いることができる。
  (a) 軍艦及び軍隊輸送船
  (b) 総トン数 500 トン未満の貨物船
  (c) 機械的推進手段を有していない船舶
  (d) 原始的な木造船
  (e) ヨット（旅客定員 12 人以下のもの）
  (f) 貿易に従事しないプレジャーヨット
  (g) 漁船
  (h) 特定の海域で用いられる浮体施設（すなわち，FPSO，FSU 等）

-2. 本章の規定は，次の**(1)**及び**(2)**に掲げるシステム及びインターフェースに適用する。

(1) 船上の運用技術（OT）システム。すなわち，物理的プロセスを制御又は監視するためにデータを用いるコンピュータシステムであって，サイバーインシデントに対して脆弱になることがあり，侵害された場合には，人の安全及び船舶の安全にとって危険な状況並びに／又は環境に対する脅威に導きうるものに適用する。特に，次に掲げる船舶の機能及びシステムの運用に用いられるコンピュータシステムについては，船上に備えられている場合，考慮しなければならない。
  (a) 推進
  (b) 操舵
  (c) 投錨及び係留
  (d) 発電及び分電
  (e) 火災探知及び消火システム
  (f) ビルジ及びバラストシステム，積付計算機
  (g) 水密性及び浸水検知
  (h) 照明（例えば，非常灯，低位置，航海灯等）
  (i) 要求される安全システムであって，当該システムの途絶又は機能障害が船舶の運用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，圧力容器の安全システム，ガス検知システム等）
  (j) 条約により要求される航海設備
  (k) 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
  航海設備及び通信システムについては，本章の要件に適合することを条件に，**4.4** において要求されるセキュリティ機能に代えて，*IEC* 61162-460 又は他の同等の規格を適用することを，本会が認めることがある。
  (l) その他本会が必要と認めるもの

(2) 本章の適用対象であるコンピュータシステムとそれ以外のシステムとの間にある，すべてのインターネットプロ

トコル（IP）ベースの通信インターフェース。ここでいう「それ以外のシステム」には，少なくとも次に例示するものが含まれる。

(a) 旅客又は訪船者のサービス又は管理システム
(b) 旅客用ネットワーク
(c) 事務用ネットワーク
(d) 船員の福祉用システム
(e) その他すべてのシステムであって，恒久的又は（例えば保守作業中に）一時的に OT システムに接続されるもの

4.1.3 限定

システムのハードウェアの耐環境性能及びソフトウェアの機能については，本章に規定していない。本章に加えて，次に掲げる要件にもよらなければならない。

(1) システムのハードウェアの耐環境性能について，**D 編 18.7.1** により要求される場合には，同**(1)**の要件
(2) ソフトウェアの機能に関する機器の安全性について，**3.1.1** により適用される場合には，**3 章**の要件

4.2 定義及び略語の説明

4.2.1 用語

本章における用語の定義は，次の**(1)**から**(27)**による。

(1) 「攻撃対象領域」とは，不正ユーザーがシステムにアクセスして，影響を与える又はデータを引き抜くことができうるすべての点の集合をいう。攻撃対象領域は，デジタル的なもの及び物理的なものの 2 つの分類から構成される。デジタル的な攻撃対象領域には，組織のネットワークに接続するすべてのハードウェア及びソフトウェアが含まれる。ここには，アプリケーション，コード，ポート，サーバー及びウェブサイトが含まれる。物理的な攻撃対象領域は，デスクトップコンピュータ，ハードドライブ，ノートパソコン，携帯電話，取外し可能なドライブ及び不用意に破棄されたハードウェアのような，攻撃者が物理的にアクセスできるすべての端末から構成される。
(2) 「認証」とは，主張された特性が正当なものであることの保証を提供することをいう。
(3) 「補完的対策」とは，1 又は複数の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採用される別の解決策をいう。
(4) 「コンピュータシステム」とは，情報の収集，処理，保守，使用，共有，発信，処分等，1 つ以上の定められた目的を達成するために組織化されたプログラム可能な電子デバイス又は相互運用できる複数のプログラム可能な電子デバイスをいう。船上のコンピュータシステムには，情報技術(IT)及び運用技術(OT)のシステムが含まれる。また，コンピュータシステムは，ネットワークを介して接続されたサブシステムの組合せである場合もある。船上のコンピュータシステムは，直接又は公共の通信手段（インターネット等）を介して，陸上のコンピュータシステム，他船のコンピュータシステム及び／又は他の施設と接続されることもある。
(5) 「コンピュータネットワーク」とは，合意された通信プロトコルにより電子的にデータ通信する目的で，2 以上のコンピュータ間を接続することをいう。
(6) 「管理策」とは，ポリシー，手順，指針，慣行又は組織構造を含む，リスク管理手段をいう。管理的，技術的，経営的又は法的なものがある。
(7) 「サイバーインシデント」とは，意図して又は意図せず，船上の 1 又は複数のコンピュータシステムを標的とした若しくは当該コンピュータシステムに影響を及ぼす，攻撃的サイバー操作の結果として生じるイベントであって，船上のシステム，ネットワーク及びコンピュータ又はそれらが処理，保存又は伝送する情報に対して実際に又は潜在的に悪影響を与え，被害を低減するための対応措置を必要としうるものをいう。サイバーインシデントには，船上のコンピュータシステムにおいて生成，記録又は使用される情報又は当該コンピュータシステムに接続されたネットワーク上の情報に対する不正アクセス，悪用，改ざん，破壊又は不適切な開示が含まれる。サイバーインシデントには，システムの故障は含まれない。
(8) 「サイバーレジリエンス」とは，船舶の安全運航のために使用される運用技術（OT）の混乱又は障害に起因し，人の安全若しくは船舶の安全にとって危険な状況又は環境に対する脅威に潜在的につながるインシデントの発生を低減し影響を軽減する機能をいう。
(9) 「多層防御」とは，組織の役割及び複数の層にまたがる可変的な防壁を確立するための，人，技術及び運用機能を

統合した情報セキュリティ戦略をいう。

(10) 「不可欠なシステム」とは，推進及び操舵並びに船舶の安全に不可欠なサービスの提供に寄与するコンピュータシステムをいう。不可欠なサービスは，「主たる不可欠なサービス」と「二次的に不可欠なサービス」から構成される。「主たる不可欠なサービス」とは，推進及び操舵を維持するために連続運転が必要なサービスをいう。「二次的に不可欠なサービス」とは，推進及び操舵を維持するために必ずしも連続運転が必要ではないが，船舶の安全を維持するために必要なサービスをいう。

(11) 「ファイアウォール」とは，あらかじめ定義されたルールによって制御される，入出力のネットワークトラフィックを監視及び制御する論理的又は物理的な防壁をいう。

(12) 「ファームウェア」とは，電子デバイスに組み込まれたソフトウェアであって，工業製品及びシステムの制御，監視及びデータ操作を担うものをいう。通常，これらは自己完結しており，ユーザーが操作のためにアクセスすることはできない。

(13) 「ハードニング」とは，攻撃対象領域を減らすことにより，システムの脆弱性を軽減する行為をいう。

(14) 「情報技術（IT)」とは，運用技術（OT）とは対照的に，データを情報として利用することに焦点を当てたデバイス，ソフトウェア及び関連するネットワークをいう。

(15) 「統合されたシステム」とは，1 又は複数の特定の目的を達成するために構成された，相互に作用する多数のサブシステム及び／又は機器を組み合わせたシステムをいう。

(16) 「ネットワークスイッチ（スイッチ)」とは，パケット交換により，データの受信，処理及び送り先のデバイスへの送信を行って，デバイス同士をコンピュータネットワーク上で接続するデバイスをいう。

(17) 「攻撃的サイバー操作」とは，OT 又は IT システムの拒否，劣化，混乱，破壊又は操作をもたらす行為をいう。

(18) 「運用技術（OT)」とは，船上のシステムを監視及び制御するためのデバイス，検知器，ソフトウェア及び関連するネットワークをいう。物理的プロセスの制御又は監視のためにデータを利用することに焦点を当てたものを OT システムとみなすことができる。

(19) 「OT システム」とは，制御，警報，監視，安全又は内部通信機能を提供するコンピュータシステムをいう。

(20) 「パッチ」とは，セキュリティ上の脆弱性及びバグに対処するため又はオペレーティングシステム若しくはアプリケーションを改善するために，インストールされたソフトウェアやデータをアップデートするよう設計されたソフトウェアをいう。

(21) 「プロトコル」とは，ネットワーク上のコンピュータが通信するために使用する，共通のルール及び信号の組合せをいう。プロトコルによりデータ通信，ネットワーク管理及びセキュリティを行うことができる。船上のネットワークは，通常，TCP/IP スタックに基づくプロトコル又は様々なフィールドバスを実装している。

(22) 「復旧」とは，レジリエンスの計画を維持し，また，サイバーセキュリティイベントによって損なわれた機能又はサービスを回復するための，適切な活動の開発及び実行をいう。復旧の機能は，サイバーセキュリティイベントによる影響を軽減するために，通常運転への迅速な復帰をサポートする。

(23) 「供給者」とは，システム又はサブシステムとして動作するアプリケーション，組み込み機器，ネットワーク機器，ホスト機器等により構成される，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（ハードウェア又はソフトウェア)の製造者又はプロバイダをいう。供給者は，システム統合者にプログラム可能な機器，サブシステム又はシステムを提供する責任がある。

(24) 「システム」とは，1 又は複数の特定の目的を達成するために構成された，相互に作用するプログラム可能なデバイス及び／又はサブシステムの組合せをいう。

(25) 「システムの分類 (I, II, III)」とは，**3.3.1** で定義された，システムの機能への影響に基づくシステムの分類をいう。

(26) 「統合者」とは，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，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，船舶が引き渡されるまでは造船所によって担われなければならない。

(27) 「信頼できないネットワーク」とは，本章の適用対象外のネットワークをいう。

4.3 セキュリティの考え方

4.3.1 システム及び機器

-1. システムは，安全で保護された信頼できるプロセスの実行を可能にするハードウェア及びソフトウェアで構成することができる。典型例として，機関制御システム，自動船位保持設備（DPS）等がある。

-2. 機器には，次に掲げるものが含まれる。

(1) ネットワークデバイス（すなわち，ルーター，マネージドスイッチ）

(2) セキュリティデバイス（すなわち，ファイアウォール，IDS／侵入検知システム）

(3) コンピュータ（すなわち，ワークステーション，サーバー）

(4) 自動化デバイス（すなわち，PLC／プログラマブルロジックコントローラー）

(5) クラウド上の仮想マシン

4.3.2 サイバーレジリエンス

4.4.2 及び **4.4.3** に規定するサイバーレジリエンスに関する要件は，**5 章**の適用対象範囲にあるすべてのシステムに適用される。信頼できないネットワークとのインターフェースに関する追加要件は，そのような接続が設計されるシステムにのみ適用される。

4.3.3 不可欠なシステムの可用性

-1. 不可欠なシステムについてのセキュリティ対策は，当該システムの可用性に悪影響を及ぼすものであってはならない。

-2. セキュリティ対策の実行は，安全機能の喪失，制御機能の喪失，監視機能の喪失又は健康，安全及び環境に被害を及ぼす可能性のある保護の喪失を引き起こすものであってはならない。

-3. 当該システムは，船舶が業務遂行に必要な運用を継続できるように，船舶並びにそのシステム，人員及び貨物の安全のために必要なデータの機密性，完全性及び可用性を確保するよう，適切に設計されたものでなければならない。

4.3.4 補完的対策

-1. 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。

-2. 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。

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

次に掲げる図書を，本章に規定する要件に従って本会に提出されなければならない。**4.6.2** も参照すること。

(1) コンピュータシステム資産インベントリ

各コンピュータシステムについて，資産に関するインベントリには以下の情報を含まなければならない。

(a) ハードウェアコンポーネントリスト（例えば，ホスト機器，組込機器，ネットワーク機器）

i) 名称

ii) ブランド／製造者

iii) モデル／型式

iv) 機能／目的の簡潔な説明

v) 物理的インターフェース（例えば，ネットワーク，シリアル）

vi) システムソフトウェアの名前／型式（例えば，オペレーティングシステム，ファームウェア）

vii) システムソフトウェアのバージョン及びパッチレベル

viii) 対応している通信プロトコル

(b) ソフトウェアコンポーネントリスト(例えば,アプリケーションソフトウェア,ユーティリティソフトウェア)

i) ソフトウェアがインストールされているハードウェアコンポーネント

ii) ブランド／製造者

iii) モデル／型式

iv) 機能／目的の簡潔な説明

v) ソフトウェアのバージョン

(2) トポロジー図

(a) 物理トポロジー図は，システムの物理的な構成を図示しなければならない。当該図は，コンピュータシステム資産インベントリ中のハードウェアコンポーネントを特定できるようにしなければならない。また，当該図は以下を図示しなければならない。

i) 全てのエンドポイント及びネットワーク機器（冗長化されたユニットの識別を含む）

ii) I/O ユニットとの通信を含む通信ケーブル（ネットワーク，シリアルリンク等）

iii) その他のネットワーク又はシステムとの通信ケーブル

(b) 論理トポロジー図は，システム内のコンポーネント間のデータフローを図示しなければならない。また，当該図は以下を図示しなければならない。

i) 通信エンドポイント（例えば，ワークステーション，コントローラー，サーバー）

ii) ネットワーク機器（スイッチ，ルーター，ファイアウォール）

iii) 物理コンピュータ及び仮想コンピュータ

iv) 物理通信パスと仮想通信パス

v) 通信プロトコル

(c) 要求されるすべての情報が明確に図示されている場合，物理トポロジー図及び論理トポロジー図をまとめたものとしても差し支えない。

(3) セキュリティ機能仕様書

(a) 当該説明は，ハードウェア及びソフトウェアコンポーネントを備えたコンピュータシステムが，**4.4.2** に要求するセキュリティ機能をどのように満足するかに関して記載しなければならない。

(b) 本章の適用範囲内にあるコンピュータシステムに対する，あらゆるネットワークインターフェースを記載しなければならない。これには，通信先のコンピュータシステム，データフロー及び通信プロトコルを含めなければならない。統合者が通信先のコンピュータシステムを他のセキュリティゾーンに割り当てている場合には，セキュリティゾーン境界の保護を担うコンポーネント（**5.4.3(2)(a)**参照）について，それがコンピュータシステムの一部として納入されるならば，詳細に記載しなければならない。

(c) 本章の適用範囲外にあるシステム又は外部のネットワークに対するあらゆるネットワークインターフェース（信頼されていないネットワーク）を記載しなければならない。これには，**4.4.3** に要求する追加セキュリティ機能への準拠を明記し，乗組員への関連する手順又は指示を含めなければならない。セキュリティゾーン境界の保護を担うコンポーネント（**5.4.3(2)(a)**参照）について，それがコンピュータシステムの一部として納入されるならば，詳細に記載しなければならない。

(d) 要求事項ごとに，別の章として示さなければならない。システム内の全てのハードウェア及びソフトウェアコンポーネントは，説明の中で関連するものとして扱われなければならない。

(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策ではないこと。

iv) より高いセキュリティリスクを発生させないこと。

(f) 要求事項への準拠を確認するために必要な補足資料（例えば，OEM 情報）は，説明文中で参照し，提出しなければならない。

(4) セキュリティ機能試験要領書

(a) 当該方案は，システムが **4.4.2** 及び **4.4.3** の要求事項に準拠していることを，試験によりどのように実証するかを説明しなければならない（補完的対策を含む）。分析的評価による適合の実証試験にあっては，特別に検討されることがある。当該方案には，適用されるそれぞれの要件について章立てして記載し，以下についても含めなければならない。

i) 必要な試験条件（すなわち，期待される試験結果が再現される試験を行うことができることを確保すること。）

ii) 試験機器

iii) 初期条件
iv) 試験方法論，詳細な試験手順
v) 期待される試験結果及び合格基準

(b) 当該方案は，試験中に試験結果をアップデートし，所見を記録する手段を含むこと。

(5) セキュリティ構成指針

(a) 当該指針は，セキュリティ機能の推奨設定を説明し，デフォルト値を特定しなければならない。この目的は，**5 章**及び統合者による仕様（例えば，ユーザーアカウント，権限，パスワードポリシー，機器の安全状態，ファイアウォールルール等）に従って，セキュリティ機能が実装されていることを確保することである。

(b) 当該指針は，**表 X4.1** 中 **29** の検証の根拠となるものである。

(6) セキュア開発ライフサイクル文書

当該文書は，要求に応じて本会に提出され，**4.5** のセキュア開発ライフサイクルに関する要求事項に従った供給者のプロセス及び管理策の記述を含むものでなければならない。また，ソフトウェアのアップデート及びパッチの適用について記載しなければならない。当該文書は，**2.2.2-5.**に基づく本会の検査のために準備されなければならない。

(7) コンピュータシステムの保守・検証手順書

当該計画は，要求に応じて本会に提出され，システムのセキュリティ関連の保守及び試験に関する手順を含むものでなければならない。当該計画は，**表 X4.1** 中 **19** で要求する，システムのセキュリティ機能のあるべき動作をユーザーが確認する方法についての指示を含むものでなければならない。

(8) 船主のインシデント対応とリカバリープランをサポートする情報

当該情報は，要求に応じて本会に提出され，ユーザーが以下を達成することを可能にする手順又は指示を含むものでなければならない。

(a) ローカル独立制御（**5.4.5(2)**）
(b) ネットワークの分離（**5.4.5(3)**）
(c) 監査記録によるフォレンジック（**表 X4.1** 中 **13** 参照）
(d) あらかじめ決定した出力（**5.4.5(4)**及び**表 X4.1** 中 **20** 参照）
(e) バックアップ（**表 X4.1** 中 **26** 参照）
(f) 復旧（**表 X4.1** 中 **27** 参照）
(g) 制御されたシャットダウン，リセット，ロールバック，再起動（**5.4.6(3)**）

(9) 変更管理手順書

当該手順書は，要求に応じて本会に提出されなければばらない。当該手順書は，サイバーセキュリティに特化したものではなく，**3 章**で要求されているものを参考にすることができる。

(10) 供給者による試験報告書

本章のセキュリティ機能を満たす，使用承認の証明書を有するコンピュータシステムは，本会による検査を免除することができる。ただし，供給者が署名した試験報告書は，供給者が設計，建造，試験，設定及びハードニングが完了していることを実証するものとし，本会は検査において当該報告書の確認を行う（**4.6.3** 及び **2.2.3** 参照）。

4.4.2 要求されるセキュリティ機能*

表 X4.1 に掲げるセキュリティ機能は，**4.1.2** に規定する適用範囲内にあるすべてのコンピュータシステムに対して要求される。**表 X4.1** に掲げる要求事項は，*IEC* 62443-3-3 の中から選択された要件に基づいている。各要件の完全な内容，根拠及び関連するガイダンスを決定するために，読者は当該規格を参照する必要がある。ここで，**表 X4.1** 中にいう「*IEC* 62443-3-3/SR x.x」（x には数字が入る）とは，次に掲げる *IEC* 規格に定める SR (System requirement)のうち，該当するものに関連することを示すものである。

IEC 62443-3-3:2013（産業用通信ネットワーク，ネットワーク及びシステムセキュリティ，第 3-3 部 : システムセキュリティ要求事項及びセキュリティレベル）

4.4.3 追加で要求されるセキュリティ機能

-1. **表 X4.2** に掲げる追加で要求されるセキュリティ機能は，信頼できない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（すなわち，本章の適用範囲外にあるすべてのネットワークとのインターフェース）に対して要求される。ここで，**表 X4.2** 中にいう「*IEC* 62443-3-3/SR x.x」（x には数字が入る。以下同じ。）が示す内容は，**4.4.1** にいうものと同様である。また，「*IEC* 62443-3-3/SR x.x, RE x.x」とは，当該 SR (System requirement)に関する RE (Requirement

enhancement)のうち，該当するものに関連することを示すものである。

-2. セキュリティゾーンの境界を通過して通信するコンピュータシステムにあっては，**5.4.3(1)**及び**(2)**に規定するネットワークセグメント化及びゾーン境界の保護に関する要件も満たさなければならない。

表 X4.1　　要求されるセキュリティ機能

番号	対象	要件
認証されていないエンティティによる意図しないアクセスからの保護		
1	人間のユーザーの識別及び認証	コンピュータシステムは，直接又はインターフェースを介してシステムにアクセス可能なすべての人間のユーザーを識別及び認証するものでなければならない。 (*IEC* 62443-3-3/SR 1.1)
2	アカウントの管理	コンピュータシステムは，権限を有するユーザーによるすべてのアカウントの管理（アカウントの追加，有効化，変更，無効化及び削除を含む）をサポートする機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 1.3)
3	識別子の管理	コンピュータシステムは，ユーザー，グループ及び役割による識別子の管理をサポートする機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 1.4)
4	認証コードの管理	コンピュータシステムは，次に掲げる機能を提供するものでなければならない。 ・　認証コードの内容の初期化 ・　制御システムのインストールに際しての，すべてのデフォルト認証コードの変更 ・　すべての認証コードの変更／アップデート ・　保存及び伝送されるすべての認証コードの，不正開示及び変更からの保護 (*IEC* 62443-3-3/SR 1.5)
5	無線アクセスの管理	コンピュータシステムは，無線通信をするすべてのユーザー（人，ソフトウェアプロセス又はデバイス）を識別及び認証する機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 1.6)
6	パスワードによる認証の強度	コンピュータシステムは，パスワードの設定を，最短の長さ及び文字の種類の多様性に基づいて，強化する機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 1.7)
7	認証時のフィードバック	コンピュータシステムは，認証プロセス中のフィードバックを，明確でないものにしなければならない。 (*IEC* 62443-3-3/SR 1.10)
意図しない誤使用からの保護		
8	権限付与の実施	すべてのインターフェースにおいて，人間のユーザーに，職務分離及び最小特権の原則に従って権限を割り当てられるものでなければならない。 (*IEC* 62443-3-3/SR 2.1)
9	無線の使用の管理	コンピュータシステムは，一般に受け入れられるセキュリティに関する業界の慣行に従って，システムへの無線接続の認可，監視及び使用制限を実施する機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 2.2)
10	可搬式及び携帯用デバイスの使用の管理	可搬式及び携帯用デバイスの使用に対応したコンピュータシステムは，次に掲げる機能を含むものでなければならない。 ・　可搬式及び携帯用デバイスの使用は，設計上許可されたものだけに制限すること。 ・　可搬式及び携帯用デバイスへ／からのコード及びデータの転送を，制限すること。 (*IEC* 62443-3-3/SR 2.3)
11	モバイルコード	コンピュータシステムは，Java スクリプト，ActiveX 及び PDF のようなモバイルコードの使用を制御するものでなければならない。 (*IEC* 62443-3-3/SR 2.4)

12	セッションロック	コンピュータシステムは，設定可能な無操作時間の経過後又は手動によるセッションロックの有効化後に，更なるアクセスを防止することが可能なものでなければならない。 (*IEC* 62443-3-3/SR 2.5)
13	監査可能なイベント	コンピュータシステムは，少なくとも次に掲げるイベントについて，セキュリティに関連する監査記録を作成するものでなければならない：アクセス制御，オペレーティングシステムのイベント，バックアップ及び復元のイベント，設定の変更，通信の喪失 (*IEC* 62443-3-3/SR 2.8)
14	監査用の記憶容量	コンピュータシステムは，監査記録の記憶容量を，ログ管理に関する一般に認識された推奨に従って割り当てる機能を提供できるものでなければならない。監査の仕組みは，当該容量を超過する可能性を下げるように実装されなければならない。 (*IEC* 62443-3-3/SR 2.9)
15	監査プロセスの不具合への対応	コンピュータシステムは，監査プロセスの不具合発生時に，不可欠なサービス及び機能の喪失を防ぐ機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 2.10)
16	日時の記録	コンピュータシステムは，監査記録に日時を記録するものでなければならない。 (*IEC* 62443-3-3/SR 2.11)
意図しない操作からのコンピュータシステムの完全性の保護		
17	通信の完全性	コンピュータシステムは，伝送される情報の完全性を保護するものでなければならない。 (*IEC* 62443-3-3/SR 3.1)
18	悪意のあるコードからの保護	コンピュータシステムは，悪意のあるコードや不正なソフトウェアによる影響を防止，検知及び低減するための適切な保護手段を実行する機能を提供できるものでなければならない。また，保護の仕組みをアップデートする機能を有するものでなければならない。 (*IEC* 62443-3-3/SR 3.2)
19	セキュリティ機能の検証	コンピュータシステムは，セキュリティ機能のあるべき動作の検証をサポートし，また，保守中に発生した異常を報告する機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 3.3)
20	あらかじめ決定した出力	コンピュータシステムは，攻撃により通常の動作を維持できなくなった場合に，出力をあらかじめ指定した状態に設定する機能を提供するものでなければならない。あらかじめ指定した状態とは，次に掲げるものとすることができる。 - 非使用時の状態 - 最後の既知の値，又は - 固定値 (*IEC* 62443-3-3/SR 3.6)
盗聴や意図しない漏洩による不正な情報流出の防止		
21	情報の機密性	コンピュータシステムは，読取りに関して明示的な承認が求められる情報について，保管時であるか伝送中であるかにかかわらず，機密性を保護する機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 4.1)
22	暗号の使用	暗号を使用する場合，コンピュータシステムは一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従って，暗号アルゴリズム，鍵の長さ及び仕組みを使用するものでなければならない。 (*IEC* 62443-3-3/SR 4.3)

コンピュータシステムの運用状況の監視及びインシデントへの対応		
23	監査ログへのアクセス	コンピュータシステムは，権限を有する人及び／又はツールによる読取り専用での監査ログへのアクセスの機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 6.1)
通常の稼働状況下において，制御システムが確実に動作することの確保		
24	サービス拒否攻撃からの保護	コンピュータシステムは，DoS イベント発生中にも，不可欠な機能を維持するための最小限の機能を提供するものでなければならない。 注 : DoS 事象発生中に，コンピュータシステムは縮退モードで動作して差支えないが，それが危険な状況を招くものであってはならない。過負荷による DoS 事象，すなわち，ネットワークの容量を超えさせたりコンピュータのリソースを消費させたりする試みが考慮されなければならない。 (*IEC* 62443-3-3/SR 7.1)
25	リソースの管理	コンピュータシステムは，リソースを使い果たさないように，セキュリティ機能によるリソースの利用を制限する機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 7.2)
26	システムのバックアップ	コンピュータシステムは，通常の運用に影響することなく，重要なファイルの識別及び場所特定並びにユーザーレベル及びシステムレベルでの情報（システム状態に関する情報を含む）のバックアップ実施をサポートするものでなければならない。 (*IEC* 62443-3-3/SR 7.3)
27	システムの復旧及び再構成	コンピュータシステムは，混乱又は故障の後，既知の保護された状態に復旧及び再構成される機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 7.4)
28	代替電源	コンピュータシステムは，既存のセキュリティ状態又は文書化された縮退モードに影響することなく，代替電源へ及び代替電源から切り替える機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 7.5)
29	ネットワーク及びセキュリティ構成設定	コンピュータシステムのトラフィックは，供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能を提供するものでなければならない。コンピュータシステムは，現在用いられているネットワーク及びセキュリティ構成の設定へのインターフェースを提供するものでなければならない。 (*IEC* 62443-3-3/SR 7.6)
30	最小限の機能性	次に掲げるもののインストール，可用性及びアクセス権は，コンピュータシステムが提供する機能の厳格な要求に限られなければならない。 ・オペレーティングシステムソフトウェアのコンポーネント，プロセス及びサービス ・ネットワークサービス，ポート，プロトコル，ルート及びホストへのアクセス並びにすべてのソフトウェア (*IEC* 62443-3-3/SR 7.7)

表 X4.2　　追加で要求されるセキュリティ機能

番号	対象	要件
31	人間のユーザーの多要素認証	信頼できないネットワークから又は当該ネットワークを経由してコンピュータシステムにアクセスする場合，人間のユーザーには多要素認証が要求される。 (*IEC* 62443-3-3/SR 1.1, RE 2)
32	ソフトウェアプロセス及びデバイスの識別及び認証	コンピュータシステムは，ソフトウェアプロセス及びデバイスを識別及び認証するものでなければならない。 (*IEC* 62443-3-3/SR 1.2)
33	失敗したログイン試行	コンピュータシステムは，一定時間内における信頼できないネットワークからの連続した無効なログイン試行の制限を実施するものでなければならない。 (*IEC* 62443-3-3/SR 1.11)
34	システム使用通知	コンピュータシステムは，認証前にシステム使用通知メッセージを表示する機能を提供するものでなければならない。システム使用通知メッセージは，権限を有する人員により設定可能でなければならない。 (*IEC* 62443-3-3/SR 1.12)
35	信頼できないネットワーク経由のアクセス	信頼できないネットワークから又は当該ネットワークを経由してのコンピュータシステムへのすべてのアクセスは，監視及び管理されなければならない。 (*IEC* 62443-3-3/SR 1.13)
36	アクセス要求の明示的な承認	コンピュータシステムは，船上にいる権限を有する人員により明示的に承認された場合を除き，信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否するものでなければならない。 (*IEC* 62443-3-3/SR 1.13, RE1)
37	リモートセッションの終了	コンピュータシステムは，設定可能な無操作時間の経過後に自動で又はセッションを開始したユーザーが手動で，リモートセッションを終了する機能を提供するものでなければならない。 (*IEC* 62443-3-3/SR 2.6)
38	暗号化による完全性の保護	コンピュータシステム は，信頼できないネットワークとの又は当該ネットワークを経由した通信中における情報の変更を認識するために，暗号化の仕組みを採用するものでなければならない。 (*IEC* 62443-3-3/SR 3.1, RE1)
39	入力の検証	コンピュータシステムは，プロセス制御の入力として使用される又はコンピュータシステムの動作に直接影響する，信頼できないネットワーク経由のすべての入力データにつき，構文，長さ及び内容を検証するものでなければならない。 (*IEC* 62443-3-3/SR 3.5)
40	セッションの完全性	コンピュータシステムは，セッションの完全性を保護するものでなければならない。無効なセッション ID は，拒否されなければならない。 (*IEC* 62443-3-3/SR 3.8)
41	セッション終了後のセッション ID の無効化	コンピュータシステムは，ユーザーのログアウト又はその他のセッション終了（ブラウザセッションを含む）に伴い，セッション ID を無効化するものでなければならない。 (*IEC* 62443-3-3/SR 3.8, RE1)

4.5 セキュア開発ライフサイクルに関する要件

4.5.1 提出資料

-1. システム又は機器の開発は，次に掲げる段階におけるセキュリティ面について幅広く扱ったセキュア開発ライフサイクル（SDLC／Secure Development Lifecycle）によらなければならない。

(1) 要件分析段階
(2) 設計段階
(3) 実装段階
(4) 検証段階
(5) リリース段階
(6) 保守段階
(7) 終了段階

-2. 上述の段階においてセキュリティ面をどのように扱ったかを記録した文書が作成されなければならない。また，当該文書は少なくとも以下の **4.5.2** から **4.5.8** に規定する管理されたプロセスを統合するものでなければならない。当該文書は，審査及び承認用に本会に提出されなければならない。ここで，各条にいう「*IEC* 62443-4-1」及びそれに続く記載は，次に掲げる *IEC* 規格に定める SM (Security management), SUM (Security update management)又は SG (Security guidelines)についての記載のうち，該当するものに関連することを示すものである。

IEC 62443-4-1:2018（産業用オートメーション及び制御システムのセキュリティ，第 4-1 部：安全な製品開発ライフサイクル要求事項）

4.5.2 秘密鍵の管理策（*IEC* 62443-4-1/SM-8)

製造者は，該当する場合，コード署名に使用する秘密鍵を不正アクセス又は改ざんから保護するための手順上及び技術上の管理策を保有しなければならない。

4.5.3 セキュリティアップデートの文書（*IEC* 62443-4-1/SUM-2）

製品のセキュリティアップデートに関する文書であって，少なくとも次に掲げる内容を含むものが，（サイバーセキュリティ連絡窓口の設置又はユーザーがアクセス可能な定期的発行物等を通じて）ユーザーに入手可能となることを確保するプロセスが採用されなければならない。

(1) セキュリティパッチが適用される製品のバージョン番号
(2) 承認されたパッチの手動及び自動プロセス経由による適用方法に関する説明
(3) 製品にパッチを適用することで発生する可能性のある影響（再起動を含む）の記述
(4) 承認されたパッチが適用されたことの確認方法に関する説明
(5) パッチを適用しないこと並びに資産所有者が承認又は導入しないパッチに使用できるメディエーションに関するリスク

4.5.4 依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書（*IEC* 62443-4-1/SUM-3)

依存するコンポーネント又はオペレーティングシステムのセキュリティアップデートに関する文書であって，ユーザーが利用可能となることを保証するプロセスが採用されなければならない。当該文書にあっては，少なくとも，製品が依存するコンポーネント又はオペレーティングシステムのセキュリティアップデートに対応しているかどうかの記載を含むこと。

4.5.5 セキュリティアップデートの配信（*IEC* 62443-4-1/SUM-4)

サポート対象であるすべての製品及び製品バージョンに対するセキュリティアップデートが，セキュリティパッチが真正であることを検証できる方法で，製品ユーザーに入手可能となることを確保するプロセスが採用されなければならない。製造者は，アップデートについてリリース前に試験するための QA プロセスを有さなければならない。

4.5.6 製品の多層防御（*IEC* 62443-4-1/SG-1）

製品に関する文書であって，製品のインストール，運用及び保守をサポートするために，セキュリティに関する多層防御の戦略を記述したものを作成するプロセスが存在しなければならない。当該文書は，次に掲げる内容を含むものでなければならない。

(1) 製品が実装するセキュリティ機能，また，多層防御の戦略におけるその役割
(2) 多層防御の戦略によって対処される脅威

(3) レガシーコードに関連するリスクを含む，製品に関連する既知のセキュリティリスクに対する，製品ユーザーの緩和策

4.5.7 環境において期待される多層防御策 (*IEC* 62443-4-1/SG-2)

製品ユーザーに関する文書であって，製品が使用される外部の環境から提供されることが期待されるセキュリティに関する多層防御の手段を記述したものを作成するプロセスが採用されなければならない。

4.5.8 セキュリティハードニング指針 (*IEC* 62443-4-1/SG-3)

製品ユーザーに関する文書であって，製品のインストール時及び保守時における製品のハードニングの指針を含むものを作成するプロセスが採用されなければならない。当該指針は，少なくとも，次に掲げるものに関する指示，根拠及び推奨事項を含むものでなければならない。

(1) 製品（第三者のコンポーネントを含む）と，製品のセキュリティコンテキストとの統合
(2) 製品のアプリケーションプログラミングインターフェース／プロトコルと，ユーザーアプリケーションとの統合
(3) 製品の多層防御の戦略の適用及び維持
(4) ローカルセキュリティポリシーをサポートするセキュリティオプション／機能の設定及び使用，また，それぞれのセキュリティオプション／機能に関する次に掲げる事項
  (a) 製品の多層防御の戦略への貢献
  (b) 設定可能な値及びそのデフォルト値の記述であって，それぞれがセキュリティにどのように作用して，実用上どのような影響を及ぼし得るかを含むもの
  (c) 値の設定，変更及び削除
(5) セキュリティ関連のすべてのツール及びユーティリティに関する指示及び推奨事項であって，製品のセキュリティの管理，監視，インシデント処理及び評価をサポートするもの
(6) 定期的なセキュリティ保守活動のための指示及び推奨事項
(7) 製品に関するセキュリティインシデントを供給者へ報告することについての指示
(8) 製品の保守及び管理に関するセキュリティ上のベストプラクティスについての記述

4.6 適合の実証

4.6.1 導入

-1. 供給者は，統合者と協力して，コンピュータシステムに本章が必須であるかどうかを判断しなければならない。（**図 X4.1** 参照）

-2. セキュリティ要件への適合は，**図 X4.2** に示すように実証されなければならない。また，この分類プロセスは船舶ごとに異なるが，最終的にシステムの証明書を取得しなければならない。

-3. **船用材料・機器等の承認及び認定要領第 7 編 10 章**に基づく使用承認は任意であり，標準的かつ定常的に製造されるコンピュータシステムに適用される。システム認証及び使用承認の定義については，**3.2.1** 及び **3.2.2** を参照すること。

-4. **図 X4.1** 及び **X4.2** のプロセスは，航海設備及び無線設備について，他の同等の規格を適用する場合にも適用される。（**4.1.2** 参照）この場合，**図 X4.1** は，（本章に代えて）同等の規格が必須かどうかを示しており，**図 X4.2** は，コンピュータシステムが同等の規格に従って使用承認されている場合，認証プロセスが軽減されることを示している。

図 X4.1 適用の判断

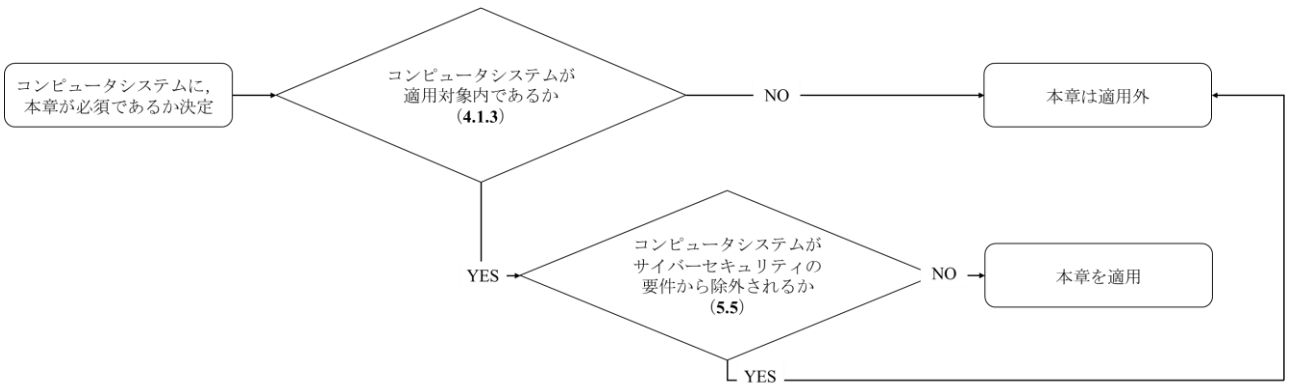
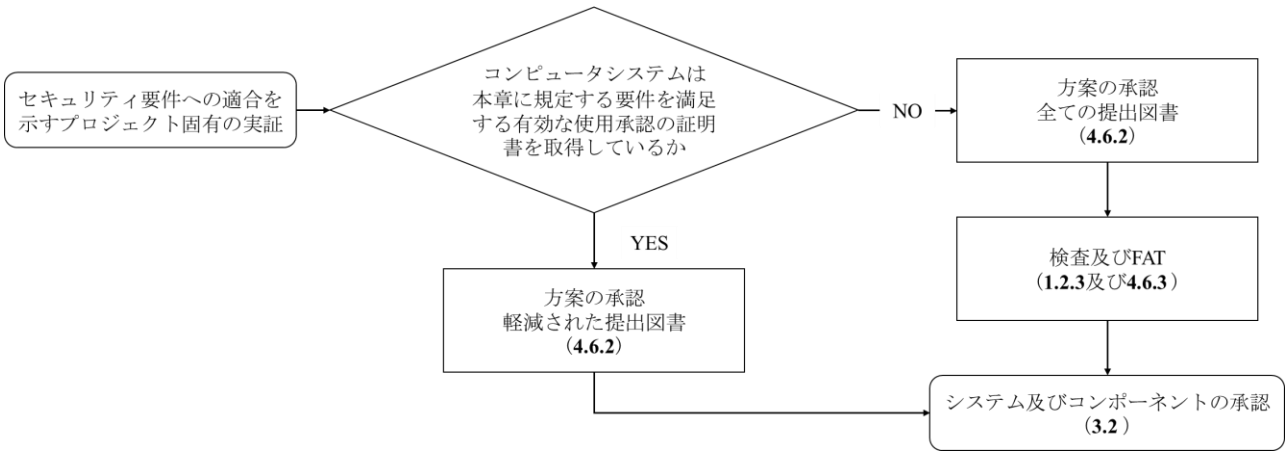


図 X4.2　　セキュリティ要件への適合



4.6.2　　提出資料の承認

-1.　提出資料の承認は，特定の船舶を対象としたコンピュータシステムの文書の審査による。**2.2.3** に規定する文書は供給者によって提出される。当該文書は，本章に規定する要求事項への適合を本会が確認可能なものでなければならない。

-2.　コンピュータシステムが，本章に規定する要求事項を満足する有効な使用承認の証明書を保持している場合，本会の承認を得て，船舶の特定の書類一式を削減したものを本会に提出することができる（**表 X2.3** 参照）。

-3.　承認された文書は，統合者へのコンピュータシステムの納品に含まれなければならない。

4.6.3　　製造工場等における試験

-1.　製造工場等における試験は，本章の要求事項を満たす有効な使用承認の証明書を保有しないコンピュータシステムに要求される，個船毎の検証試験である。

-2.　製造工場等における試験の目的は，試験及び／又は分析評価により，コンピュータシステムが本章の要件に適合していることを実証することである。検査及び製造工場等における試験は，供給者の施設または試験及び検査のための適切な装置を有する他の事業所で実施されなければならない。

-3.　提出資料の承認及び製造工場等における試験の完了後，本会が発行する証明書は，統合者への引き渡しの際に，コンピュータシステムとともに納められなければならない。

5章　船舶のサイバーレジリエンス

5.1　一般

5.1.1　目的*

-1　本章の狙いは，サイバーレジリエントな船舶に導く技術的手段を利害関係者に提供することを目的として，船舶のサイバーレジリエンスに関する最低限の要件を提供することである。

-2.　本章は，サイバーレジリエンスに関する集合体としての船舶を対象としており，船上のシステム，機器及びコンポーネントのサイバーレジリエンスに関する他の要件及び業界標準を適用することにより補完される土台となることが意図されたものである。

-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最低要件は，**4章**に規定されている。

5.1.2　適用

-1.　本章の規定は，**4章**が適用されるコンピュータシステムに適用する。

-2.　本章が想定するサイバーインシデントは，**5.2** に定義するとおり，船上の OT システムを標的としたすべての攻撃的操作の結果であるイベントである。

5.1.3　システムの分類

システムの分類は，システムの不具合が人の安全及び船舶の安全並びに／又は環境への脅威にもたらす結果に基づいて，**3.3.1** に定義されている。

5.1.4　コンピュータシステム及びサイバーレジリエンスに関する関連規定

本章に加えて，次に掲げる関連規定にも注意すること。

(1)　**3章**「コンピュータシステム」

(2)　**4章**「船上のシステム及び機器のサイバーレジリエンス」

(3)　*IACS* Recommendation No.166「サイバーレジリエンスに関する勧告」（*IACS* Recommendation No.166 は，サイバーレジリエントな船舶であって，そのレジリエンスを一生にわたって維持することが可能であるものの建造を支援するために，利害関係者が参照及び適用することができる，推奨される非強制の技術要件である。サイバーレジリエンスに関する *IACS* Recommendation No.166 は，その発行後に建造契約が行われた船舶用であり，また，その発行前に既に就航している船舶にも参考として用いることができる。本章が強制要件として適用される船舶に対して本章及び *IACS* Recommendation No.166 の両方を用いる際は，同じ項目に関する要件において両者に差異がある場合には，本章の要件を優先しなければならない。）

5.2　定義

5.2.1　用語*

本章における用語の定義は，次の**(1)**から**(23)**に定めるところによる。

(1)　「年次検査」とは，**B編 3章**に規定する検査で船体，機関，艤装及び消火設備等の一般現状について確認する検査をいう。

(2)　「攻撃対象領域」とは，不正ユーザーがシステムにアクセスして，影響を与えたりデータを引き抜いたりすることができうるすべての点の集合をいう。攻撃対象領域には，デジタル的なもの及び物理的なものの 2 つがある。デジタル的な攻撃対象領域には，組織のネットワークに接続するすべてのハードウェア及びソフトウェアが含まれる。ここには，アプリケーション，コード，ポート，サーバー及びウェブサイトが含まれる。物理的な攻撃対象領域には，デスクトップコンピュータ，ハードドライブ，ノートパソコン，携帯電話，取外し可能なドライブ及び不用意に破棄されたハードウェアのような，攻撃者が物理的にアクセスできるすべての端末が含まれる。

(3)　「認証」とは，主張された特性が正当なものであることの保証を提供することをいう。

(4)　「補完的対策」とは，1 又は複数の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採用される別の解決策をいう。

(5)　「コンピュータシステム」とは，情報の収集，処理，保守，使用，共有，発信，処分等，1 つ以上の定められた目

的を達成するために組織化されたプログラム可能な電子デバイス又は相互運用できる複数のプログラム可能な電子デバイスをいう。船上のコンピュータシステムには，情報技術(IT)及び運用技術(OT)のシステムが含まれる。また，コンピュータシステムは，ネットワークを介して接続されたサブシステムの組合せである場合もある。船上のコンピュータシステムは，直接又は公共の通信手段（インターネット等）を介して，陸上のコンピュータシステム，他船のコンピュータシステム及び／又は他の施設と接続されることもある。

(6) 「サイバーインシデント」とは，意図して又は意図せず，船上の 1 又は複数のコンピュータシステムを標的とした若しくは当該コンピュータシステムに影響を及ぼす，攻撃的サイバー操作の結果として生じるイベントであって，船上のシステム，ネットワーク及びコンピュータ又はそれらが処理，保存又は伝送する情報に対して実際に又は潜在的に悪影響を与え，被害を低減するための対応措置を必要としうるものをいう。サイバーインシデントには，船上のコンピュータシステムにおいて生成，記録又は使用される情報又は当該コンピュータシステムに接続されたネットワーク上の情報に対する不正アクセス，悪用，改ざん，破壊又は不適切な開示が含まれる。サイバーインシデントには，システムの故障は含まれない。

(7) 「サイバーレジリエンス」とは，船舶の安全運航のために使用される運用技術（OT）の途絶又は障害に起因し，人の安全及び船舶の安全にとって危険な状況並びに／又は環境に対する脅威に潜在的につながるインシデントの発生を低減し影響を軽減する機能をいう。

(8) 「不可欠なサービス」とは，推進及び操舵並びに船舶の安全のためのサービスをいう。不可欠なサービスは，「主たる不可欠なサービス」と「二次的に不可欠なサービス」から構成される。「主たる不可欠なサービス」とは，推進及び操舵を維持するために連続運転が必要なサービスをいう。「二次的に不可欠なサービス」とは，推進及び操舵を維持するために必ずしも連続運転が必要ではないが，船舶の安全を維持するために必要なサービスをいう。

(9) 「情報技術（IT）」とは，運用技術（OT）とは対照的に，データを情報として利用することに焦点を当てたデバイス，ソフトウェア及び関連するネットワークをいう。

(10) 「統合されたシステム」とは，1 又は複数の特定の目的を達成するために構成された，相互に作用する多数のサブシステム及び／又は機器を組み合わせたシステムをいう。

(11) 「論理的ネットワークセグメント」とは，「ネットワークセグメント」と同様であるが，2 以上の論理的ネットワークセグメントが同じ物理的コンポーネントを共有するものをいう。

(12) 「ネットワーク」とは，合意された通信プロトコルにより電子的にデータ通信を行うことを目的とした，2 以上のコンピュータ間の接続をいう。

(13) 「ネットワークセグメント」とは，本章においては，OSI 参照モデルの第 2 層のイーサネットのセグメント（ブロードキャストドメイン）をいう。

(14) 「運用技術（OT）」とは，船上のシステムを監視及び制御するためのデバイス，検知器，ソフトウェア及び関連するネットワークをいう。物理的プロセスの制御又は監視のためにデータを利用することに焦点を当てたものを OT システムとみなすことができる。

(15) 「物理的ネットワークセグメント」とは，「ネットワークセグメント」と同様であるが，物理的コンポーネントを，他のネットワークセグメントと共有しないものをいう。

(16) 「プロトコル」とは，ネットワーク上のコンピュータが通信するために使用する，共通のルール及び信号の組合せをいう。プロトコルにより，データ通信，ネットワークの管理及びセキュリティを実行することができる。船上のネットワークは，通常，TCP/IP スタック又は様々なフィールドバスに基づくプロトコルを実装している。

(17) 「セキュリティゾーン」とは，本章の適用範囲内にあって，同一のセキュリティ要件に適合するコンピュータシステムの集合をいう。それぞれのゾーンは，アクセス制御ポリシーが適用される単一又は複数のインターフェースによって構成される。

(18) 「船主／会社」とは，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個人をいう。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。

(19) 「定期検査」とは，**B 編 5 章**に規定する検査で船体，機関，艤装及び消火設備等について行う詳細な検査をいう。

(20) 「供給者」とは，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。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。

(21) 「統合者」とは，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。

(22) 「信頼できないネットワーク」とは，本章の適用対象外のネットワークをいう。

(23) 「ロールバック」とは，システムを以前の状態に戻す操作をいう。

5.3 目的及び要件の構成

5.3.1 最上位の目的

-1. 最上位の目的は，サイバーリスクに対して運用上レジリエントで，安全・安心な海運を支えることである。

-2. 安全・安心な海運は，効果的なサイバーリスク管理システムを通じて達成することができる。サイバーリスクに対してレジリエントで，安全・安心な海運を支えるための，サイバーリスクの管理に関する目的を，5.3.2 に示す 5 つの機能要素ごとに規定する。

5.3.2 機能要素ごとの目的

以下に示す目的及び関連する機能要素は，並列的なものであり，単一の包括的なリスク管理の枠組みの一部として考えられるべきである。

(1) 識別

船上のシステム，人員，資産，データ及び機能に対するサイバーセキュリティ上のリスクを管理するために，組織的な理解を深める。

(2) 防御

船舶をサイバーインシデントから保護し，船舶の運航の継続性を最大化するための，適切な防護策を開発及び実装する。

(3) 検知

船上におけるサイバーインシデントの発生を検知及び識別するための，適切な手段を開発及び実装する。

(4) 対応

船上における検知されたサイバーインシデントに関して行動を起こすための，適切な手段及び活動を開発及び実装する。

(5) 復旧

サイバーインシデントにより障害が発生した，船舶の運航に不可欠なすべての機能又はサービスを復元するための，適切な手段及び活動を開発及び実装する。

5.3.3 要件の構成

本章に規定する要件は，次に示すように構成されている。

(1) 要件は，ゴールベースアプローチに従って構成されている。

(2) 5.3.2 に示す機能要素ごとの目的を達成するために，機能要件／技術的要件が規定されている。

(3) 要件は，許容可能な程度のレジリエンスを実現でき，運航上のリスク及び OT システムの複雑さに関わらず，すべての船級船／ユニットに対して適用することにより，利害関係者が統一的に実装でき，すべての船種に適用可能とすることが意図されている。

(4) それぞれの要件について，根拠が示されている。

(5) 取るべき行動及び利用可能とすべき書類の概要についても，船舶の一生におけるそれぞれの段階ごとに，関連する利害関係者と共に示している。

5.4 船舶のサイバーレジリエンスの要件

5.4.1 一般

本章に含まれているのは，5.3.1 に規定する最上位のゴールを達成するために満足すべき要件を，5.3.2 に規定する 5 つの機能要素に従って整理したものである。要件は，船舶の設計，建造及び運航に関わる利害関係者によって，満足されなければならない。利害関係者としては，次に掲げるものがある（定義については 5.2 参照）。上述の要件は，これらの利害関係者によって満たされうるが，本章の目的のために要件を満たす責任は，本会と契約を結んだ利害関係者が有する。

(1) 船主／会社
(2) 統合者
(3) 供給者
(4) 本会

5.4.2 識別

識別の機能要素に関する要件は，一方では，船上のコンピュータシステム，それらの相互依存性及び関連する情報フローについてであり，もう一方では，それらの管理，運用及びガバナンスに関わるキーリソース並びにそれらの役割及び責任について識別することを目的としている。

(1) 船舶資産インベントリ

(a) 要件

本章の適用範囲内にあるコンピュータシステムのハードウェア及びソフトウェア（アプリケーションプログラム，オペレーティングシステム，もしあればファームウェア及びその他のソフトウェアコンポーネントを含む）並びに当該コンピュータシステム同士で及び船上若しくは陸上にあるその他のコンピュータシステムと繋ぐネットワークのインベントリが提供され，船舶の一生にわたってアップデートされなければならない。

(b) 根拠

船上のコンピュータシステム及び OT システムに用いられるソフトウェアのインベントリは，船舶のサイバーレジリエンスを効果的に管理するうえで不可欠である。その主な理由は，すべてのコンピュータシステムが潜在的な脆弱性のポイントになるからである。サイバー犯罪者は，管理されていない旧式のハードウェア及びソフトウェアを，システムへの不正侵入に悪用することがある。それに加えて，コンピュータシステム資産の管理により，船舶の安全上の目標に対する各システムの重要性について，会社が理解することができる。

(c) 要件の詳細

船舶資産インベントリは，5.1.2-1.に掲げるコンピュータシステムが船内に存在する場合には，少なくともそれらを含むものでなければならない。当該インベントリは，船舶の一生にわたってアップデートされ続けなければならない。ソフトウェア及びハードウェアの改造であって新たな脆弱性をもたらしうるもの又は機能的な依存性若しくはシステム間の接続の変更は，インベントリに記録されなければならない。機密情報（例えば，IP アドレス，プロトコル，ポート番号）がインベントリに含まれる場合には，当該情報へのアクセスを，権限を与えられた者だけに限定するための特別な措置が講じられなければならない。

i) ハードウェア

1) 本章の適用範囲内にあるすべてのハードウェアデバイスに関して，船舶資産インベントリは，少なくとも 4.4.1(1)に示す情報を含むものでなければならない。

2) 加えて，船舶資産インベントリには，コンピュータシステムに関するシステムの分類及びセキュリティゾーンを規定することができる。

ii) ソフトウェア

1) 本章の適用範囲内にあるすべてのソフトウェア（例えば，アプリケーションプログラム，オペレーティングシステム，ファームウェア）に関して，船舶資産インベントリは，少なくとも，4.4.1(1)に示す情報を含むものでなければならない。

2) 本章の適用範囲内にあるコンピュータシステムのソフトウェアは，船舶のサイバーセキュリティ・レジリエンス計画書に含まれる，ソフトウェアの保守及びアップデートの管理に関するポリシーによる船主のプロセスに従い，保守及びアップデートされなければならない（2.2.3-5.(7)参照）。

(d) 適合の実証

i) 設計段階

1) システム統合者は，船舶資産インベントリを本会に提出しなければならない。（2.2.3-4.参照）

2) 船舶資産インベントリは，本章の適用範囲内にあるすべての個別のコンピュータシステムの資産インベントリを含むものでなければならない。また，システム統合者によって納入される本章の適用範囲内にあるあらゆる設備についても，船舶資産インベントリに含まれなければならない。

ii) 建造段階

統合者は，船舶資産インベントリをアップデートし続けなければならない。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)参照）を提出し，また，以下について実証しなければならない。

1) 船舶資産インベントリがアップデートされ，引渡し時に完成されていること。

2) 本章の適用範囲内にあるにコンピュータシステムが，船舶資産インベントリに正確に反映されていること。

3) 本章の適用範囲にあるコンピュータシステムのソフトウェアがアップデートされ続けること。（例えば，脆弱性スキャン又はコンピュータシステム起動時のソフトウェアのバージョンの確認による。）

iv) 運用段階

1) 運用段階における検査の一般要件については，2.2.3-5.を参照すること。

2) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，本章の適用範囲内にあるコンピュータシステムの変更管理のプロセスを記載しなければならない。

－ 変更管理（2.2.3-5.）

－ ハードウェア及びソフトウェアの改造（5.4.2(1)(c)）

3) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，ソフトウェアアップデートの管理について記載しなければならない。

－ 脆弱性及びサイバーリスク（5.4.2(1)(b)及び(c)）

－ セキュリティパッチ（5.4.3(6)(c)iii)2)）

4) 初回の年次検査

船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

－ 承認された変更管理のプロセスが遵守されていること。

－ コンピュータシステムのソフトウェアについて，既知の脆弱性及び機能的な依存性が考慮されていること。

－ 船舶資産インベントリがアップデートされ続けていること。

5) 2 回目以降の年次検査

船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明しなければならない。

6) 定期検査

船主は，船舶サイバーレジリエンス試験要領書に従って，5.4.2(1)(d)iii)に規定する事項を本会に実証しなければならない。

5.4.3 防御*

防御の機能要素に関する要件は，起こりうるインシデントの影響を制限する又は封じ込める能力を支える適切な防護策の開発及び実装を目的としている。

(1) セキュリティゾーン及びネットワークセグメント

(a) 要件

i) 本章の適用範囲内にあるすべてのコンピュータシステムは，明確に定義されたセキュリティポリシー及びセキュリティ機能を伴うセキュリティゾーンにグループ化されなければならない。セキュリティゾー

ンは，隔離する（すなわち，エアギャップ）か，又は，ゾーン間のデータ通信を管理する手段（例えば，ファイアウォール／ルーター，単方向シリアルリンク，TCP/IP ダイオード，ドライ接点等）を用いて他のセキュリティゾーン若しくは他のネットワークと接続しなければならない。

ii) セキュリティゾーンの境界を超えることができるのは，明示的に許可されたトラフィックに限定されなければならない。

(b) 根拠

i) ファイアウォールにより境界を防御しても，入ってくるトラフィックを監視するための侵入検知システム（IDS／Intrusion Detection Systems）又は侵入防御システム（IPS／Intrusion Prevention Systems）を加えても，境界を突破することは常に可能である。ネットワークのセグメント化により，攻撃者がネットワーク全体を攻撃することは困難になる。

ii) セキュリティゾーン及びネットワークのセグメント化による主な利点は，攻撃対象領域の広がりを抑え，攻撃者がシステム内を横方向に移動できることを防ぎ，ネットワークのパフォーマンスを向上させることにある。コンピュータシステムをセキュリティゾーンに割り当てる概念により，コンピュータシステムをリスクの特性に従ってグループ化できる。

(c) 要件の詳細

i) 1 のセキュリティゾーンに，複数のコンピュータシステム及びネットワークを含めることができるが，それらはすべて本章及び **4 章**に規定するセキュリティ要件に適合可能なものでなければならない。

ii) セキュリティゾーンのネットワークは，他のゾーン又はネットワークから，論理的又は物理的にセグメント化されなければならない。**5.4.3(6)(c)**も参照すること。

iii) 要求される安全機能を提供するコンピュータシステムは，分離されたセキュリティゾーンにグループ化され，かつ，他のセキュリティゾーンから物理的にセグメント化されなければならない。

iv) 航海設備及び通信システムは，機関又は貨物システムと同じセキュリティゾーンに含めてはならない。航海設備及び／又は無線通信システムが他の同等の基準（**4.1.2-2.(1)(k)**参照）に従って承認されている場合，これらのシステムは専用のセキュリティゾーンにあるべきである。

v) 無線機器は，専用のセキュリティゾーンになければならない。**5.4.3(5)**も参照すること。

vi) 本章の適用対象に含まれないシステム，ネットワーク又はコンピュータシステムは，信頼できないネットワークとみなされ，本章により要求されるセキュリティゾーンから物理的にセグメント化されなければならない。あるいは，これらの OT システムがセキュリティゾーンに求められるものと同じ要件に適合する場合には，当該システムをセキュリティゾーンに含めることができる。

vii) セキュリティゾーン内のコンピュータシステムの主要な機能に影響することなく，セキュリティゾーンを隔離することが可能でなければならない。（**5.4.5(3)**参照）

(d) 適合の実証

i) 設計段階

1) 統合者は，ゾーン及びコンジット図並びにサイバーセキュリティデザインの説明を提出しなければならない（**2.2.3-3.(4)**及び**(5)**参照）。

2) ゾーン及びコンジット図は，本章の適用範囲内にあるコンピュータシステム及びそれらがどのようにセキュリティゾーンにグループ化されているかを図示し，次の情報を含むものでなければならない。

— セキュリティゾーンの明確な表示。

— 本章の適用範囲内にあるコンピュータシステムの簡略化した図，当該コンピュータシステムが割り当てられているセキュリティゾーンの表示及びコンピュータシステム／機器の物理的場所の表示。

— 供給者によって提供されたコンピュータシステムのシステムトポロジー図に関する，承認されたバージョンへの参照（**4.4.1(2)**）。

— セキュリティゾーン内のシステム間のネットワーク通信を示す図。

— 異なるセキュリティゾーンにあるシステム間のネットワーク通信（コンジット）を示す図。

— セキュリティゾーン内のシステムと信頼できないネットワークとの通信（コンジット）を示す図。

3) 統合者は，サイバーセキュリティデザインの説明に，次の情報を含めなければならない。

— セキュリティゾーンに割り当てられたコンピュータシステムに関する短い説明。それぞれのコン

ピュータシステムがゾーン及びコンジット図において，識別可能でなければならない。

－ 同一のセキュリティゾーン内のコンピュータシステム間のネットワーク通信。説明は，通信の目的及び特徴（すなわち，プロトコル及びデータフロー）を含むものでなければならない。

－ 異なるセキュリティゾーンにあるコンピュータシステムのネットワーク通信。説明は，通信の目的及び特徴（すなわち，プロトコル及びデータフロー）を含むものでなければならない。また，ゾーン境界にあるデバイス及び当該ゾーン境界の通過が許可されるトラフィックの特定（例えば，ファイアウォールルール）を含むものでなければならない。

－ セキュリティゾーン内のコンピュータシステムと信頼できないネットワークとのすべての通信。説明は，離散信号及びシリアル通信並びに IP ベースのネットワーク通信の目的及び特徴（すなわち，プロトコル及びデータフロー）を含むものでなければならない。また，ゾーン境界にあるデバイス及び当該ゾーン境界の通過が許可されるトラフィックの特定（例えば，ファイアウォールルール）を含むものでなければならない。

ii) 建造段階

統合者は，ゾーン及びコンジット図をアップデートし続けなければならない。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，また，以下について実証しなければならない。

1) 船上のセキュリティゾーンが承認された文書（すなわち，ゾーン及びコンジット図，サイバーセキュリティデザインの説明，船舶資産インベントリ並びに供給者から提供された関連文書）に従って実装されていること。これは，例えば，物理的な設備の検査，ネットワークスキャン及び／又は，設置された機器が承認された設計に従ってセキュリティゾーンにグループ化されていることを検査員が確認できるその他の方法によって行うことができる。

2) セキュリティゾーン境界は，承認されたサイバーセキュリティデザインの説明に記載されたトラフィックのみを許可すること。これは，ファイアウォールルールの評価，ポートスキャン等によって行うことができる。

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書にセキュリティゾーン境界にあるデバイス（例えば，ファイアウォール）の管理について記載しなければならない。

－ 最小権限の原則（**5.4.3(2)(a)**）

－ 明示的に許可されたトラフィック（**5.4.3(1)(a)**）

－ サービス拒否（DoS）事象に対する防御（**5.4.3(2)(a)**）

－ セキュリティ監査記録の審査（**5.4.4(1)(c)**）

2) 初回の年次検査

船主は，ゾーン及びコンジット図がアップデートされ続けていることを本会に実証し，また，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわちセキュリティゾーン境界が上述の要件に従って管理されていることを示さなければならない。

3) 2 回目以降の年次検査

船主は，本会の要請に応じて、初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

4) 定期検査

船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する行動を本会に実証しなければならない。

(2) ネットワークを防御する防護策

(a) 要件

i) セキュリティゾーンは，**5.1.1** の規定に従って，ファイアウォール又は同等の手段により防御されなければならない。

ii) 当該ネットワークは，過度なデータフローレートの発生や，ネットワークリソースのサービスの質を低下させうるその他のイベントからも，防御されなければならない。

iii) 本章の適用範囲内にあるコンピュータシステムは，最小権限の原則に従って実装されなければならない。すなわち，不要な機能，ポート，プロトコル及びサービスを無効化又は禁止することにより，不可欠でない機能の使用を禁止又は制限し，不可欠な機能のみを備えるように構成されなければならない。

(b) 根拠

i) ネットワークの防御は，ネットワークの完全性，機密性及び可用性を防御するように設計された多数の技術，規範及び構成に及ぶ。脅威の環境は常に変化し，攻撃者は常に脆弱性を見つけて悪用しようとする。

ii) ネットワークの防御に取り組む際には，考慮すべき多くの層がある。攻撃は，ネットワークのいずれの層でも起こりうるため，ネットワークのハードウェア，ソフトウェア及びポリシーは，それぞれの領域に対処するよう設計されたものでなければならない。

iii) 物理的及び技術的なセキュリティ管理策は，権限を与えられていない人員がネットワークコンポーネントに物理的にアクセス可能となることを防ぐように，また，ネットワーク上に保存又は伝送されるデータを保護するように策定される。一方，手順的なセキュリティ管理策は，ユーザーのふるまいを管理するセキュリティポリシー及びプロセスから成る。

(c) 要件の詳細

ネットワークの設計は，ネットワークに対して予定されたデータフローを達成すべく，また，サービス拒否（DoS）及びネットワークストーム／大量のトラフィックによるリスクを最小するための手段を含むものでなければならない。データフローレートの推定に際しては，少なくとも，ネットワークの容量，予定されたアプリケーションにより要求されるデータ速度及びデータフォーマットが考慮されなければならない。

(d) 適合の実証

i) 設計段階

要件なし。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，また，以下について実証しなければならない。なお，**2)**及び **3)**については，**2.2.3-4.(2)**に規定するコンピュータシステムの認証において実施した場合には，省略することができる。

1) ゾーン境界保護デバイスを標的とするサービス拒否（DoS）攻撃の試験（該当する場合）

2) 各ネットワークセグメント内から発信される過剰なデータ流量からの保護を確保する，サービス拒否（DoS）の試験。当該試験は，ネットワークのフラッディング（つまり，ネットワークセグメント上の使用可能な容量の消費を試みること）及びアプリケーション層への攻撃（つまり，ネットワーク内の選択されたエンドポイントの処理能力の消費を試みること）を対象とするものでなければならない。

3) 例えば，解析的評価及びポートスキャンにより，コンピュータシステムの不要な機能，ポート，プロトコル及びサービスが，供給者によって提供されたハードニング指針に従って削除又は禁止されていることの試験。**4.5.8** 及び **2.2.2-5.(7)**を参照すること。

iv) 運用段階

1) 運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

2) 定期検査

コンピュータシステムに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(3) 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

(a) 要件

本章の適用範囲内にあるコンピュータシステムは，ウイルス，ワーム，トロイの木馬，スパイウェア等のような，悪意のあるコードに対して防御されなければならない。

(b) 根拠

i) ユーザーに知られずにシステムに侵入するウイルス又はすべての望まれざるプログラムは，自己複製及び拡散し，システムのパフォーマンス，ユーザーのデータ／ファイルに影響する悪意のある望まれざる行動を起こし，及び／又はデータセキュリティの手段を回避することがある。

ii) ウイルス対策，マルウェア対策，スパム対策のソフトウェアは，警備員付きの閉じたドアのように，侵入してくる悪意のあるウイルスを防御するよう予防的に機能する。多くの場合はウイルスがシステムに危害を加える前に，ウイルスである可能性のあるものを検知して除去する。

iii) 悪意のあるコードがコンピュータシステムに侵入する一般的な手段は，電子メール，その添付ファイル，ウェブサイト，取外し可能な媒体（例えば，USB デバイス，フロッピーディスク又は CD），PDF 文書，ウェブサービス，ネットワーク接続及び感染したノートパソコンである。

(c) 要件の詳細

i) マルウェアからの防御は，本章の適用範囲内にあるコンピュータシステムに実装されなければならない。業界標準のウイルス対策及びマルウェア対策ソフトウェアであって最新版に維持されているものが利用可能なオペレーティングシステムを有するコンピュータシステムには，ウイルス対策及び／又はマルウェア対策ソフトウェアをインストール，保守及び定期的にアップデートしなければならない。ただし，コンピュータシステムが有する，要求される機能及びサービスレベル（例えば，リアルタイムでタスクを実行する分類 II 及び III のコンピュータシステム）を提供する能力が，当該ソフトウェアをインストールすることにより損なわれる場合を除く。

ii) ウイルス対策及びマルウェア対策のソフトウェアがインストールできないコンピュータシステムには，運用手順，物理的防護策又は製造者の推奨に従う形の，マルウェアからの防御が実装されなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，次の情報を含めなければならない。

1) 各コンピュータシステムについて，悪意のあるコード又は不正ソフトウェアから保護するために供給者によって提供されたメカニズムであって承認されたものの概要。

2) マルウェア対策ソフトウェアを有するコンピュータシステムについて，当該ソフトウェアをアップデートし続ける方法に関する情報。

3) 運用上の条件又は船主の管理システムに実装することが必要である物理的な防護策。

ii) 建造段階

統合者は，建設段階においてマルウェア対策がアップデートされ続けることを確保しなければならない。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，また，以下について実証しなければならない。なお，当該要件は，**2.2.3-4.(2)**に規定するコンピュータシステムの認証において実施した場合には，省略することができる。

1) 承認されたマルウェア対策ソフトウェア又はその他の補完的対策が有効であること。（例えば，信頼できるマルウェア対策テストファイルによる試験）。

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，マルウェアからの防御に関する管理について記載しなければならない。

— 保守／アップデート（**5.4.3(3)(c)**）

— 運用手順，物理的防護策（**5.4.3(3)(c)**）

— 携帯用，可搬式，取外し可能なメディアの使用（**5.4.3(4)(c)iv)**及び **5.4.3(7)(c)**）

－ アクセス制御（5.4.3(4)）

2) 初回の年次検査

船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

－ マルウェア対策ソフトウェアが保守及びアップデートされていること。

－ 携帯用，可搬式又は取外し可能なデバイスの使用に関する手順が守られていること。

－ アクセス制御に関するポリシー及び手順が守られていること。

－ 物理的防護策が維持されていること。

3) 2 回目以降の年次検査

船主は，本会の要請に応じて、初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

4) 定期検査

船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(4) アクセス制御

(a) 要件

本章の適用範囲内にあるコンピュータシステム及びネットワークは，当該システムと通信若しくは相互作用したり，データ処理のためにシステムリソースを使用したり，システムに含まれるデータに関する知識を得たり又はシステムのコンポーネント及び機能を制御したりするための能力及び手段を選択的に制限するような，物理的及び／又は論理的／デジタルの手段を備えるものでなければならない。当該手段は，最小権限の原則に従ったアクセスのレベルに応じて人員がコンピュータシステムにアクセスする能力を，妨げるものであってはならない。

(b) 根拠

i) 攻撃者は，船舶のシステム及びデータへのアクセスを，船上で，会社内で又はインターネット接続を介して遠隔で，試みることがある。このため，船舶及び積荷の安全を確保するために，コンピュータ関連の資産やネットワーク等への物理的及び論理的なアクセス制御を実装すべきである。

ii) 物理的脅威及び関連する対策は，ISPS コードにおいても考慮されている。同様に，ISM コードにも，船舶の安全運航及び環境保護を確保するための指針が含まれている。ISPS 及び ISM コードの履行により，安全上重要な資産へのアクセス制御に関する指示及び手順を船舶保安計画書（SSP）及び安全管理システム（SMS）に含めるということになりうる。

(c) 要件の詳細

本章の適用範囲内にあるコンピュータシステム及びネットワーク並びに当該システムに保存されるすべての情報へのアクセスは，責任又は予定された職務の一部としての情報へのアクセスの必要性に基づいて，権限を与えられた人員に対してのみ許可されるものでなければならない。

i) 物理的アクセス制御

一般に，分類 II 及び分類 III のコンピュータシステムは，不正アクセスを防ぐため，通常時に施錠可能な部屋若しくは管理されたスペースに備えるか，又は，施錠可能な棚若しくはコンソールに備えなければならない。ただし，そのような場所又は棚／コンソールは，効果的で効率的な船舶の運航を妨げないよう，設置，統合，保守，修理，交換，廃棄等のためにコンピュータシステムにアクセスする必要のある船員及び様々な利害関係者が容易にアクセスできるものでなければならない。

ii) 訪船者のための物理的アクセス制御

官庁，技術者，代理人，港湾当局者及び船主代表といった訪船者が，乗船中に船上のコンピュータシステムへアクセスすることは，例えば監督下でのみアクセスを許可することにより，制限されなければならない。

iii) ネットワークアクセスポイントへの物理的アクセス制御

分類 II 及び／又は分類 III のコンピュータシステムに接続される船上ネットワークへのアクセスポイントは，（例えば文書印刷のために）監督下で又は文書化された手順に従って接続する場合を除き，物理的及

び／又は論理的に阻止されなければならない。訪船者から一時的な接続を求められた場合（例えば文書印刷のために）には，すべての船上ネットワーク又はゲスト専用ネットワーク若しくは旅客の娯楽用ネットワークといったその他のネットワークから隔離された，独立のコンピュータが使用されなければならない。

iv) 取外し可能な媒体の制御

取外し可能な媒体の使用に関するポリシーが，取外し可能な媒体のマルウェアについての確認並びに／又はデジタル署名及び透かしによるソフトウェアの正当性の確認及び船舶のシステムへのファイルのアップロード若しくは船舶のシステムからのデータのダウンロードを許可するのに先立つスキャンに関する手順と共に，作成されなければならない。**5.4.3(7)**も参照すること。

v) クレデンシャルの管理

1) コンピュータシステム及び関連情報は，ファイルシステム，ネットワーク，アプリケーション又はデータベースに特有のアクセス制御一覧表（ACL／Access Control List）と共に保護されなければならない。船上及び陸上の人員のアカウントは，当該アカウント所有者の役割及び責任に応じて，期間限定で有効なものとしなければならず，不要になった際には削除されなければならない。

2) 船上のコンピュータシステムは，セキュリティゾーンのポリシーに適合する適切なアクセス制御により保護されていると同時に，主たる目的に悪影響を与えてはならない。強力なアクセス制御を要求するコンピュータシステムは，強力な暗号鍵又は多要素認証を用いて保護する必要がありうる。

3) 管理者特権は，会社又は船上での役割の一部として管理者特権を使用してシステムにログオンする必要のある，権限を有し適切に訓練された人員のみがコンピュータシステムにフルアクセスすることが可能となるように，アクセス制限のポリシーに従って管理されならない。

vi) 最小権限の原則

1) 本章の適用範囲内にあるコンピュータシステム及びネットワークへのアクセスが許可されるすべてのユーザー（人）には，その職務の実施に必要な最小権限のみが与えられなければならない。

2) すべての新しいアカウントの権限に関するデフォルト設定は，可能な限り低いものでなければならない。可能であれば，例えば 1 回限り使用可能なクレデンシャルで得られる期間限定の権限のみを用いるなどして，権限を高めるのは必要な短時間に限定されるべきである。時間とともに権限が蓄積することは，例えばユーザーのアカウントを定期的に監査することにより，回避されなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，コンピュータシステムの位置及び物理的アクセス制御に関する情報を含めなければならない。ここで，即時アクセスを必要とするオペレータにヒューマンマシンインターフェース（HMI）を提供するデバイスは，物理的アクセス制御のある場所に配置されていれば，ユーザーの識別及び認証を強制する必要はない。そのようなデバイスは特定されなければならない。

ii) 建造段階

統合者は，建造段階において，コンピュータシステムへの不正アクセスを防がなければならない。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，また，以下について実証しなければならない。

1) コンピュータシステムのコンポーネントが，物理的アクセスを，権限を与えられた人員だけに制御できる場所又は囲いの中に配置されていること。

2) ユーザーカウントが，職務の分離及び最小権限の原則に従って設定され，一時的なアカウントは削除されていること（**2.2.3-4.(2)**に従い，コンピュータシステムの認証に基づいて省略可能）。

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，論理的及び物理的アクセスの管理について記載しなければならない。

— 物理的アクセス制御（**5.4.3(4)(c)i)**）

— 訪船者のための物理的アクセス制御（**5.4.3(4)(c)ii)**）

－ ネットワークアクセスポイントへの物理的アクセス制御（**5.4.3(4)(c)iii)**）
－ クレデンシャルの管理（**5.4.3(4)(c)v)**）
－ 最小権限の原則（**5.4.3(4)(c)vi)**）

2) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，機密情報の管理について記述しなければならない。
－ 機密情報（**5.4.2(1)(c)**）
－ 権限を与えられた人員に許可される情報（**5.4.3(4)(c)**）
－ 無線ネットワークで送信される情報（**5.4.3(5)(c)**）

3) 初回の年次検査
船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。
－ 人員が，その責任に応じてコンピュータシステムにアクセスする権限を与えられていること。
－ 許可されたデバイスのみがコンピュータシステムに接続されていること。
－ 訪船者が，関連するポリシー及び手順に従ってコンピュータシステムにアクセスできること。
－ 物理的なアクセス制御が維持及び適用されていること。
－ クレデンシャル，鍵，機密，証明書，関連するコンピュータシステムの書類及びその他の保護すべき情報が，関連するポリシー及び手順に従って管理され，秘密が保持されていること。

4) 2 回目以降の年次検査
船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

(5) 無線通信

(a) 要件
本章の適用範囲内にある無線通信ネットワークは，次に掲げることを確保するように，設計，実装及び保守されなければならない。
i) サイバーインシデントが，他の制御システムに伝播しない。
ii) 権限を与えられたユーザー（人）のみが，無線ネットワークにアクセスできる。
iii) 権限を与えられたプロセス及びデバイスのみが，無線ネットワーク上で通信することを許可される。
iv) 無線ネットワーク上を伝送中の情報を，改ざん又は公開することができない。

(b) 根拠
i) 無線ネットワークでは，有線ネットワークと比べて，追加の又は異なるサイバーセキュリティリスクが生じる。その主な理由は，デバイスに対する物理的防御の減少及び無線周波数通信の使用である。
ii) 物理的アクセス制御が不適切であると，権限を有していない人員による物理的デバイスへのアクセスにつながることがあり，それが論理的アクセス制限の抜け道又はネットワーク上への不良なデバイスの配置につながりうる。
iii) 無線周波数における信号の伝送は，電波妨害及び盗聴に関連するリスクを生じさせ，それがピギーバッキング（侵入制限のある入り口で正規の入場者のすぐ後ろについて通り抜ける「共連れ」のこと）又はイビルツイン（本物のアクセスポイント付近に別のアクセスポイントを設置し，気付かずに接続した者の通信内容を盗聴すること）攻撃のような攻撃に悪用されうる。（https://us-cert.cisa.gov/ncas/tips/ST05-003 参照）

(c) 要件の詳細
i) 無線ネットワーク上を伝送される情報の完全性及び機密性を確保するために，業界標準及びベストプラクティスに従った暗号化アルゴリズム及び鍵の長さのような暗号化メカニズムが適用されなければならない。
ii) 無線ネットワーク上のデバイスは，無線ネットワーク上でのみ通信するものでなければならない（すなわち，両用であってはならない。）
iii) 無線ネットワークは，**5.4.3(1)**に従って分離されたセグメントとして設計され，**5.4.3(2)**に従って防御されたものでなければならない。
iv) 無線アクセスポイント及び当該ネットワーク上のその他のデバイスは，当該ネットワークへのアクセス

が制御可能なように設置及び設定されなければならない。

v) 無線通信を活用したネットワークデバイス又はシステムは，当該通信に関与するすべてのユーザー（人間，ソフトウェアプロセス又はデバイス）を識別及び認証できるものでなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，本章の適用範囲内にある無線ネットワーク及びそれらが分離されたセキュリティゾーンとしてどのように実装されているのかの説明を含めなければならない。なお，当該説明は，ゾーン境界にあるデバイス及び当該ゾーン境界の通過が許可されるトラフィックの特定を含むものでなければならない（例えば，ファイアウォールルール）。

ii) 建造段階

統合者は，建造段階において無線ネットワークへの不正アクセスを防がなければならない。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，また，以下について実証しなければならない。なお，当該要件は，**2.2.3-4.(2)**に規定するコンピュータシステムの認証において実施した場合には省略することができる。

1) 許可されたデバイスのみが無線ネットワークにアクセスできること。

2) 各供給者によって承認された文書に従って，保護された無線通信プロトコルが使用されていること（例えば，ネットワークプロトコルアナライザーツールを用いた実証による）。

iv) 運用段階

1) 運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

2) 定期検査

本章の適用範囲内にある無線ネットワークに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(6) 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

(a) 要件

本章の適用範囲内にあるコンピュータシステムは，信頼できないネットワークからの不正アクセス及びその他のサイバー上の脅威に対して，防御されたものでなければならない。

(b) 根拠

船上のコンピュータシステムはデジタル化が進み，多岐にわたる正当な機能を実行するために，インターネットへ接続されるようになった。船上のコンピュータシステムを監視及び制御するためにデジタルシステムを使用することは，サイバーインシデントに対して脆弱になる。攻撃者は，インターネット接続を通じて船上のコンピュータシステムへのアクセスを試み，コンピュータシステムの動作に影響を与える変更を加えること，コンピュータシステムの完全に制御すること，又は，コンピュータシステムから情報のダウンロードを試みることがありうる。さらに，既にサポートされていない及び／又は陳腐化したオペレーティングシステムに頼る旧式の IT 及び OT システムの使用はサイバーレジリエンスに影響するため，当該システムへの遠隔アクセスが可能である場合には，すべてのサイバーインシデントが故意の攻撃の結果とは限らないということも念頭に置いて，船上に搭載されたハードウェア及びソフトウェアが十分なレベルのサイバーレジリエンスを維持できるよう，特別な注意が払われるべきである。

(c) 要件の詳細

i) 船上の IT 及び OT システムへの遠隔アクセスの制御に関するユーザーマニュアルが作成されなければならない。明確な指針により，役割及び権限が機能について明らかにされなければならない。

ii) 本章の適用範囲内にあるコンピュータシステムの IP アドレスを，信頼できないネットワークに暴露してはならない。

iii) 信頼できないネットワークとの通信又は当該ネットワークを介した通信には，エンドポイント認証，完全性の防御並びにネットワーク層又はトランスポート層における認証及び暗号化を伴う保護された接続（例えばトンネル）が求められる。読取りの権限を必要とする情報については，機密性が確保されなければならない。

1) 設計

本章の適用範囲内にあるコンピュータシステムは，次に掲げる要件に適合しなければならない。

－ 船上の接続エンドポイントから接続を終了できるものでなければならない。船上の責任ある役割よって明示的に許可されない限り，すべての遠隔アクセスは不可能でなければならない。

－ 遠隔アクセスのセッションの中断を，OT システムの安全機能並びに OT システムで用いるデータの完全性及び可用性を損なうことなく，管理できるものでなければならない。

－ 全ての遠隔アクセスのイベントを記録し，（例えばサイバーインシデントの検知後に）遠隔接続についてオフラインで確認するのに十分な時間保持するためのログ機能を有するものでなければならない。

2) 遠隔保守に関する追加要件

保守のために遠隔アクセスを用いる場合には，前 **1)**に加えて，次に掲げる要件に適合しなければならない。

－ 陸上側と接続及び統合する方法を示す文書が船上に備えられなければならない。

－ セキュリティパッチ及びソフトウェアのアップデートは，インストールに先立って，効果的であって，かつ，許容されない副次的影響又はサイバー関連の事象を起こさないことを確保すべく，試験及び評価されなければならない。これらに関する確認報告書が，遠隔アップデートの実施に先立って，ソフトウェア供給者から入手されなければならない。

－ 供給者は，セキュリティアップデートのための計画を提供し，船主がそれを利用できるようにしなければならない（**4.5.3**，**4.5.4** 及び **4.5.5** 参照）。

－ 遠隔保守作業中，いかなる時も，権限を与えられた人員により，作業を中断及び中止し，コンピュータシステム及び関連するシステムを，以前の安全な設定にロールバックすることが可能でなければならない。

－ 範囲内にあるコンピュータシステムへの，信頼できないネットワークからのユーザー（人）によるすべてのアクセスには，多要素認証が求められる。

－ 設定可能な回数の遠隔アクセス試行が失敗した後，あらかじめ定めた時間，次の試行は阻止されなければならない。

－ 遠隔保守場所への接続が何らかの理由により中断された場合，自動ログアウト機能により，システムへのアクセスが終了されなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，次の情報を含めなければならない。

1) 本章の適用範囲内にあるコンピュータシステムであって，遠隔アクセス可能なもの又はセキュリティゾーン境界を介して信頼できないネットワークと通信するものの識別。

2) 各コンピュータシステムについて，**5.4.3(6)c)**の要件のうち該当するものへの適合に関する説明。

ii) 建造段階

統合者は，信頼できないネットワークとのあらゆる通信が，一時的にのみ有効となり，本章の要件に従って使用されることを確保しなければならない。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，以下について実証しなければならない。

1) 信頼できないネットワークとの通信は，**4.4.3** に従って保護されており，通信プロトコルが安全性の低いバージョンに変更されないこと。（例えば，ネットワークプロトコルアナライザーツールを用いた実証）

2) 遠隔アクセスには，遠隔ユーザーの多要素認証が必要であること。

3) 失敗したログイン試行の制限が実装されており，セッションが確立される前に遠隔ユーザーに通知メッセージが提供されること。

4) 遠隔接続は，船上の責任者によって明示的に許可されなければならないこと。

5) 遠隔セッションは，船上の責任者によって手動で終了できる又は一定期間非アクティブ状態の後に

自動的に終了されること。

6) 遠隔セッションはログに記録されること。（**表 X4.1** 中 **13**）

7) 指示又は手順は，各製品供給者によって提供されること。（**4.4.1(3)**参照）

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，信頼できないネットワークとの通信又は信頼できないネットワークを介した遠隔アクセス及び通信の管理について記載しなければならない。

— ユーザーマニュアル（**5.4.3(6)(c)**）

— 役割及び許可（**5.4.3(6)(c)**）

— パッチ及びアップデート（**5.4.3(6)(c)iii)2)**）

— 遠隔ソフトウェアアップデートに先立つ確認（**5.4.3(6)(c)iii)2)**）

— 中断，破棄，ロールバック（**5.4.3(6)(c)iii)2)**）

2) 初回の年次検査

船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

— 遠隔アクセスセッションは，関連するポリシー及びユーザーマニュアルに従って，記録され若しくはログが作成され，実施されていること。

— セキュリティパッチ及びその他のソフトウェアアップデートプログラムのインストールは，変更管理の手順に従って，供給者と協力して実施されていること。

3) 2 回目以降の年次検査

船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

4) 定期検査

船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(7) 携帯用及び可搬式デバイスの使用

(a) 要件

本章の適用範囲内にあるコンピュータシステムにおける携帯用及び可搬式デバイスの使用は，必要な活動のみに限定され，**表 X4.1** 中 **10** に従って管理されなければならない。これらの要件を完全に満たすことができないコンピュータシステムにあっては，インターフェースのポートが物理的にブロックされなければならない。

(b) 根拠

携帯用又は可搬式デバイス経由のマルウェア感染により，コンピュータシステムが障害を起こしうることが，一般に知られている。このため，携帯用又は可搬式デバイスの接続は，慎重に検討されるべきである。さらに，船舶の運航及び保守に用いることが求められる携帯用機器は，船主の管理下にあるべきである。

(c) 要件の詳細

携帯用及び可搬式デバイスを使用するのは，権限を与えられた人員のみでなければならず，コンピュータシステムに接続できるのは，許可されたデバイスのみでなければならない。当該デバイスの使用については，コンピュータシステムにマルウェアが侵入するリスクを考慮した，携帯用及び可搬式デバイスの使用に関する船主のポリシーに従わなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，本章の適用範囲内にあるコンピュータシステムのうち，**表 X4.1** 中 **10** の要件を満たさないもの，すなわち，ポートブロッカー等の物理的手段によりインターフェースのポートの保護を有しなければならないものに関する情報を含めなければならない。

ii) 建造段階

統合者は，コンピュータシステムにおける物理的インターフェースのポートの使用が**表 X4.1** 中 **10** に従

って制御されていること及びそのようなデバイスの使用がコンピュータシステムへのマルウェアの侵入を防ぐための手順に従っていることを確保しなければならない。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，携帯用及び可搬式デバイスの使用を制御する機能が正しく実装されていることを実証しなければならず，これに関連する次に掲げる対策を実証しなければならない。

1) 携帯用及び可搬式デバイスを使用するのは，権限を与えられた者に限られていること。
2) インターフェースのポートを使用できるのは，特定の種類のデバイスのみであること。
3) 許可されていないデバイスからは，システムにファイルを転送できないこと。
4) 許可されていないデバイス上のファイルは，自動的に実行されないこと。（自動的な実行の無効化による。）
5) ネットワークアクセスが，特定の MAC アドレス又は IP アドレスに限られていること。
6) 使用されないインターフェースのポートが，使用できない状態であること。
7) 使用されないインターフェースのポートが，物理的にブロックされていること。

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，携帯用及び可搬式デバイスの管理について記載しなければならない。
   － ポリシー及び手順（**5.4.3(4)(c)iv)**）
   － インターフェースのポートの物理的ブロック（**5.4.3(7)(a)**）
   － 権限を与えられた人員による使用（**5.4.3(7)(c)**）
   － 許可されたデバイスのみの接続（**5.4.3(7)(c)**）
   － マルウェアの侵入についてのリスクの考慮（**5.4.3(7)(c)**）
2) 初回の年次検査

   船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

   － 携帯用，可搬式又は取外し可能な媒体の使用については，権限を与えられた人員に限られ，かつ，関連するポリシー及び手順に従っていること。
   － 許可されたデバイスのみが，コンピュータシステムに接続されること。
   － 物理的なインターフェースのポートの使用を制限する手段が，承認された設計書類に従って実装されていること。
3) 2 回目以降の年次検査

   船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。
4) 定期検査

   船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

5.4.4 検知

検知の機能要素に関する要件は，船上のコンピュータシステム及びネットワーク上の異常な活動を明らかにして認識し，サイバーインシデントを識別する能力を支える適切な手段の開発及び実装を目的としている。

(1) ネットワーク動作の監視

(a) 要件

本章の適用範囲内にあるネットワークは連続的に監視されなければならず，また，故障又は機能低下の発生時には警報が発せられるものでなければならない。

(b) 根拠

サイバー攻撃は巧妙化しており，脅威に対する準備が不十分である船舶においては，建造時に知られていなかった脆弱性を標的とした攻撃がインシデントになりうる。このような知られていなかった脆弱性を標的とす

る攻撃への早期対応を可能とすべく，通常と異なる事象を検知可能な技術が必要となる。ネットワークにおける異常を検知可能であって，インシデント後の解析も可能である監視システムにより，適切に対応し，さらにサイバー関連の事象から復旧する能力が提供される。

(c) 要件の詳細

i) 本章の適用範囲内にあるネットワークを監視する手段は，次に掲げる機能を有するものでなければならない。

1) 過度のトラフィックに対する監視及び防御。
2) ネットワーク接続の監視
3) デバイス管理活動の監視及び記録
4) 許可されていないデバイスの接続に対する防御
5) ネットワーク帯域幅の使用率が，供給者が定める異常の閾値を超えた場合における，警報の作動（**3.7.2-1.**）

ii) 侵入検知システム（IDS）は，次に掲げる事項を満たす場合には，実装することができる。

1) IDS は，それぞれのコンピュータシステムの供給者により適当と認められていなければならない。
2) IDS は，受動的であって，コンピュータシステムの性能に影響しうる防御機能を作動させないものでなければならない。
3) IDS の使用者は，訓練を受けた適格な人員であるべきである。

(d) 適合の実証

i) 設計段階

要件なし。

ii) 建造段階

要件なし。

iii) 試運転段階

1) 統合者は，次に掲げるコンピュータシステムにおけるネットワークの監視及び防御の仕組みについて，船舶サイバーレジリエンス試験要領書に規定して本会に実証しなければならない。なお，当該要件は，**2.2.3-4.(2)**に規定するコンピュータシステムの認証において実施した場合には省略することができる。

－ ネットワーク接続の切断により警報が発せられ，この事象が記録されることの試験。

－ 異常に高いネットワークトラフィックが検出され，警報が発せられ，監査記録が作成されることの試験。当該試験は，**5.4.5(4)(d)iii)**に規定する試験と同時に実行して差し支えない。

－ コンピュータシステムが，ユニキャスト（1 対 1 で行われるデータ通信）メッセージ及びブロードキャスト（1 対不特定多数で行われるデータ通信）メッセージの両方を考慮して，ネットワークストーム（すなわちブロードキャストストーム，通信障害）のシナリオに安全な方法で応答することの実証（セクション **5.4.3(2)(d)iii)**も参照すること）。

－ 監査記録作成の実証（セキュリティ関連事象のログの作成）

－ 侵入検知システム（IDS）が実装されている場合，これが受動的であって，コンピュータシステムに意図された動作に影響を与えうる防御機能を作動させないことの実証。

2) 本章の適用範囲内にあるコンピュータシステムに実装される侵入検出システム（IDS）は，本会による検証を受けなければならない。関連書類が承認のために提出され，検査／試験が船上で実施されなければならない。

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，少なくとも本章中の次に掲げる要件に対処し，船舶サイバーセキュリティ・レジリエンス計画書に，コンピュータシステム及びネットワークにおける異常を検知するための管理活動を記載しなければならない。なお，当該要件は，**5.4.5(1)**に規定するインシデント対応と同時に対処することで差し支えない。

－ 異常な活動を明らかにし，認識すること（**5.4.4**）

－ セキュリティ監査記録の審査（**5.4.4(1)(c)**）

－ インシデントを検知するための指示又は手順（5.4.5(1)(a)）

2) 初回の年次検査

船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

－ コンピュータシステムが，セキュリティ監査記録の審査及びコンピュータシステムにおける警報の調査により，異常について日常的に監視されていること。

3) 2 回目以降の年次検査

船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

4) 定期検査

コンピュータシステムに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(2) 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

(a) 要件

本章の適用範囲内にあるコンピュータシステム及びネットワークは，本章にて要求されるセキュリティ機能について，性能及び機能していることを確認可能なものでなければならない。診断機能は，コンピュータシステムの完全性及び状態に関する適切な情報を予定されたユーザーに提供し，また，船舶の安全運航のための機能を維持するための手段を提供するものでなければならない。

(b) 根拠

船舶の一生にわたるサイバーレジリエンスの管理を支援するうえで，セキュリティ機能の予定された動作を検証する能力は重要である。診断機能のツールには，各デバイスの自己診断機能又はネットワーク監視ツール（例えば，ping，traceroute，ipconfig，netstat，nslookup，Wireshark，nmap 等）のような，自動又は手動の機能が含まれうる。ただし，診断機能の実行は，コンピュータシステムの動作性能に影響しうることに注意が払われるべきである。

(c) 要件の詳細

コンピュータシステム及びネットワークの診断機能は，船舶の試験及び保守段階において，要求されるすべてのセキュリティ機能の予定された動作を検証するために利用可能でなければならない。

(d) 適合の実証

i) 設計段階

要件なし。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)参照）を提出し，供給者により提供されたセキュリティ機能検証手順書の有効性を実証しなければならない。なお，当該要件は，2.2.3-4.(2)に規定するコンピュータシステムの認証において実施した場合には省略することができる。

iv) 運用段階

運用段階における検査の一般要件については，2.2.3-5.を参照すること。

1) 船主は，少なくとも本章中の次に掲げる要件に対処し，コンピュータシステム及びネットワークにおけるセキュリティ機能の正常な動作の検証に関する管理活動について，船舶サイバーセキュリティ・レジリエンス計画書に記載しなければならない。

－ 試験及び保守期間（5.4.4(2)(c)）

－ 定期的な保守（2.2.3-5.(9)）

2) 初回の年次検査

船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

－ コンピュータシステムにおけるセキュリティ機能が，定期的に試験又は検証されていること。

3) 2回目以降の年次検査

船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

5.4.5 対応

対応の機能要素に関する要件は，船上のコンピュータシステム及びネットワークに起こりうる障害の拡大を封じ込めて，サイバーインシデントの影響を最小化する能力を支える適切な手段の開発及び実装を目的としている。

(1) インシデント対応計画書

(a) 要件

インシデント対応計画書として，関連する不測の事態を取り扱い，サイバーセキュリティインシデントにどのように対応するかを規定したものが，船主によって作成されなければならない。インシデント対応計画書は，本章の適用範囲内にあるコンピュータシステムに対するインシデントについて，検知し，対応し，また，影響を制限すべく，あらかじめ定めた指示又は手順を文書化したものを含むものでなければならない。

(b) 根拠

インシデント対応計画書は，サイバーインシデント対応の責任者を手助けすることを目的とした文書である。このため，インシデント対応計画書は，簡潔に注意深く策定されると効果的である。インシデント対応計画書の作成に際しては，いかなるサイバーインシデントの重要性も理解し，それに基づいて対応策に優先順位を付けることが重要である。例えば，待機中の二重化された装置への運転切換えのような，船舶の安全運航のための機能及びサービスの程度を可能な限り維持する手段も，示されるべきである。サイバーインシデントに際しては，管理責任者（DPA）が船舶と一体となるべきである。

(c) 要件の詳細

i) 初回の年次検査までに船上に備えなければならないインシデント対応計画書の準備のための情報が，船舶の設計及び建造段階において関与した様々な利害関係者から船主に提供されなければならない。インシデント対応計画書は，船舶の運用期間にわたって（例えば保守に際して）アップデートされ続けなければならない。

ii) インシデント対応計画書は，ネットワーク上において検知されたサイバーインシデントについて，適切な官庁に通知し，インシデントに関する必要な証拠を報告し，サイバーインシデントの影響を起点となったネットワークセグメントに限定すべく時宜にかなった是正措置を講じることにより対応するための手順を提供するものでなければならない。

iii) インシデント対応計画書は，少なくとも次に掲げる情報を含むものでなければならない。なお，インシデント対応計画書は，アクセスするための電子デバイスを完全に喪失する場合に備えて，紙で備えなければならない。

1) 障害が発生したシステムを隔離するための切断点
2) 検知された進行中のサイバー事象又はサイバー事象に起因する異常な症状を伝える警報及び表示に関する説明
3) サイバーインシデントに関連して想定される主要な影響に関する説明
4) 対応の選択肢であって，シャットダウン又は独立した若しくは機側における制御への切替えに頼らないものがある場合には，それを優先したもの
5) サイバーインシデントにより故障したシステムから独立して動作させるための，独立した機側制御に関する情報（該当する場合）

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，船主がインシデント対応の計画を立てるために適用することができる，供給者から提供された情報への参照（**4.4.1(8)**参照）を含めなければならない。

ii) 建造段階

要件なし。

iii) 試運転段階

要件なし。

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，船舶サイバーセキュリティ・レジリエンス計画書に，インシデント対応計画書について記載しなければならない。当該計画書は，本章の適用範囲内にあるコンピュータシステムを取り扱い，少なくとも本章中の次に掲げる要件に対処するものでなければならない。

－ **5.4.5(1)**に規定する要件に従った，誰が，いつ，どのようにサイバーインシデントに対応するかに関する説明

－ **5.4.5(2)**に規定する要件に従った，機側／手動制御に関する手順又は指示

－ **5.4.5(3)**に規定する要件に従った，セキュリティゾーンの隔離に関する手順又は指示

－ **5.4.5(4)**に規定する要件に従った，サイバーインシデントが発生した場合に予想されるコンピュータシステムの動作に関する説明

2) 初回の年次検査

船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

－ インシデント対応計画書を，船上における責任者が利用可能であること。

－ 機側／手動制御に関する手順又は指示を，船上における責任者が利用可能であること。

－ セキュリティゾーンの切断／隔離に関する手順又は指示が，船上における責任者に利用可能であること。

－ いかなるサイバーインシデントも，インシデント対応計画書に従って対応されていること。

3) 2 回目以降の年次検査

船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

(2) 機側，独立及び／又は手動の操作

(a) 要件

SOLAS 条約第 II-1 章第 31 規則にて要求される機側におけるバックアップ制御に必要なすべてのコンピュータシステムは，主制御システムから独立したものでなければならない。ここには，効果的な機側制御に必要なヒューマンマシンインターフェース（HMI）も含まれる。

(b) 根拠

安全運航の維持に必要な機関及び機器のための独立した機側制御は，有人船における基本的な仕組みである。この要件の目的は，伝統的に，機側において手動操作を行うことにより，人員が故障及びその他のインシデントに対処可能であることを確保することにある。悪意のあるサイバー事象によるインシデントについても考慮されるべきであり，この独立した機側制御の仕組みは，その場合にも重要である。

(c) 要件の詳細

i) 機側制御及び監視のためのコンピュータシステムは，自己完結したものであって，予定された動作に関して他のコンピュータシステムとの通信に依存しないものでなければならない。

ii) 遠隔制御システム又は他のコンピュータシステムへの通信がネットワークにより行われる場合には，**5.4.3(1)**及び **5.4.3(2)**に規定するセグメント化及び防御が実装されなければならない。このことから，機側制御及び監視システムは，分離されたセキュリティゾーンであると考えなければならないということになる。以上の規定に関わらず，異なる概念を有するコンピュータシステムについては，個品ごとに特別に考慮される場合がある。

iii) 機側制御及び監視のためのコンピュータシステムは，その他の場合には，本章の要件に適合するものでなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，SOLAS 条約第 II-1 章第 31 規則に規定された機側制御が，接続された遠隔又は自動制御システムにおけるサイバーインシデントから，どのように防御されるかに関する説明を含めなければならない。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)参照）を提出し，船舶の安全のために必要な，本章の適用範囲内にあるコンピュータシステムにおいて要求される機側制御が，いかなる遠隔又は自動制御システムからも独立して操作できることを実証しなければならない。そのための試験は，機側制御システムから他のシステム／デバイスへのすべてのネットワークを切断することによって実施しなければならない。なお，当該要件は，2.2.3-4.(2)に規定するコンピュータシステムの認証において実施した場合には省略することができる。

iv) 運用段階

1) 運用段階における検査の一般要件については，2.2.3-5.を参照すること。

2) 定期検査

コンピュータシステムに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(3) ネットワークの隔離

(a) 要件

セキュリティゾーンへの又はセキュリティゾーンからの，ネットワークによる通信を，終了させることが可能でなければならない。

(b) 根拠

インシデント対応計画書には，セキュリティの突破が発生及び検知された際に，当該インシデントのさらなる拡大及び影響を防ぐための行動が含まれるであろう。当該行動は，ネットワークセグメント及び制御システムであって不可欠な機能を維持するためのものの隔離であることがある。

(c) 要件の詳細

i) インシデント対応計画書に，とるべき行動としてネットワークの隔離が示されている場合，示された手順に従って，例えば，ネットワークデバイスにある物理的な ON/OFF スイッチを操作すること又はルーター／ファイアウォールへのケーブルを外すというような類似の行動によって，セキュリティゾーンを隔離することが可能でなければならない。人員がネットワークを効率よく隔離できるように，利用可能な指示及びデバイスへの明確な表示がなければならない。

ii) 安全関連のものを含む機能及び正しい動作に影響しうる個々のシステムのデータ依存性は，不測の事態において隔離した場合にシステムにデータ又は機能的入力による埋合せを与えなければならないならばその旨を明示して，特定されなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，各セキュリティゾーンを，他のゾーン又はネットワークから隔離する方法の仕様に関する情報を含めなければならない。また，セキュリティゾーン内にあるコンピュータシステムが，他のゾーン又はネットワークから IP ネットワーク上で送信されるデータに依存していないことを実証するために，当該隔離による影響も記載されなければならない。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)参照）を提出し，セキュリティゾーン境界を通過するすべてのネットワークを切断することによって，セキュリティゾーン内にあるコンピュータシステムが他のセキュリティゾーン又はネットワークとの通信なしで適切な運用上の機能性を維持することを実証しなければならない。なお，当該要件は，2.2.3-4.(2)に規定するコンピュータシステムの認証において実施した場合には省略することができる。

iv) 運用段階

1) 運用段階における検査の一般要件については，2.2.3-5.を参照すること。

2) 定期検査

コンピュータシステムに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(4) ミニマルリスクコンディションへのフォールバック

(a) 要件

本章の適用範囲内にあるコンピュータシステム又はネットワークの，予定されているサービスを提供する能力を損なうサイバーインシデントが発生した場合には，影響を受けたシステム又はネットワークは，ミニマルリスクコンディションにフォールバックされなければならない。すなわち，生じうる安全上の問題によるリスクを減じるための安定的な停止状態に至らなければならない。

(b) 根拠

i) コンピュータシステム及び統合されたシステムの，想定外の又は対処不能な故障又はイベントに際して到達すべき 1 又は複数のミニマルリスクコンディションにフォールバックされる能力は，つじつまの合う既知の安全な状態にシステムを維持することを目的とした安全策である。

ii) ミニマルリスクコンディションへのフォールバックは，通常は，現在の動作を中止して援助の必要性を伝えるというシステムの機能を含み，また，環境条件，船舶の航海の段階（例えば，入出港中であるか外洋航行中であるか）及び発生したイベントによっても異なりうるものである。

(c) 要件の詳細

i) コンピュータシステム又はネットワークに影響するサイバーインシデントであって，予定されるサービスを要求どおりに提供するというシステムの能力を損なうものが検知され次第，システムは合理的に安全な状況に達せられる状態にフォールバックするものでなければならない。フォールバックの動作には，次に掲げるようなものが含まれる。

1) システムの完全な停止又はその他の安全な状態への移行

2) システムの切り離し

3) 制御の他のシステム又は操作者（人）への引き継ぎ

4) その他の補完的動作

ii) ミニマルリスクコンディションへのフォールバックは，船舶が安全な状態に維持される適当な時間枠内で行われなければならない。

iii) システムがミニマルリスクコンディションにフォールバックする機能は，供給者及び統合者によって，設計段階から検討されなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，本章の適用範囲内にあるコンピュータシステムの制御機能における，安全な状態に関する仕様に関する情報を含めなければならない。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，本章の適用範囲内にあるコンピュータシステムが，例えば，重要なサービスへの出力を維持しつつ操作者が代替手段によって制御及び監視機能を実行可能すること等により，（**5.4.5(4)(d)i)**に従って）安全な方法でサイバーインシデントに対応することを実証しなければならない。試験は，少なくともサービス拒否（DoS）攻撃を含むものでなければならず，また，**5.4.4(1)(d)iii)**に規定する関連する試験と同時に実行して差支えない。なお，当該要件は，**2.2.3-4.(2)**に規定するコンピュータシステムの認証において実施した場合には省略することができる。

iv) 運用段階

1) 運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

2) 定期検査

コンピュータシステムに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

5.4.6 復旧

復旧の機能要素に関する要件は，サイバーインシデントにより影響を受けた船上のコンピュータシステム及びネットワークを復元する能力を支える適切な手段の開発及び実装を目的としている。

(1) 復旧計画書

(a) 要件

復旧計画書は，本章の適用範囲内にあるコンピュータシステムを，サイバーインシデントによる途絶又は故障の後，使用可能な状態への復元を支えるために船主によって作成されなければならない。復旧計画書には，どこで誰から支援を得られるかについての詳細が，含まれなければならない。

(b) 根拠

i) インシデントへの対応手順は，システムの復旧に不可欠である。責任者は慎重に検討し，復旧の行動から推測される結果（ドライブのデータ消去等）を認識し，復旧を慎重に実行すべきである。ただし，復旧の行動は，インシデントの原因に関する貴重な情報を提供するような証拠を破壊する結果となりうることに注意すべきである。

ii) 適切である場合，運用能力を復元しつつ証拠の保存を手助けするために，外部のサイバーインシデント対応サポートを利用すべきである。

(c) 要件の詳細

i) 初回の年次検査までに船上に備えなければならない復旧計画書の準備のための情報が，船舶の設計及び建造段階において関与した様々な利害関係者から船主に提供されなければならない。復旧計画書は，船舶の運用期間にわたって（例えば保守に際して）アップデートされ続けなければならない。

ii) 復旧計画書は，船員及び外部の人員により容易に理解できるものであって，故障したシステムの復旧を確保するために不可欠な指示及び手順並びに陸上からのサポートが必要な場合にどのようにして外部からの援助を受けるかを含むものでなければならない。さらに，船上における復旧に不可欠な，ソフトウェア復旧用の媒体又はツールが利用可能でなければならない。

iii) 復旧計画書の作成に際しては，関係のある様々なシステム及びサブシステムが特定されなければならない。次に掲げる復旧の目標も規定されなければならない。

1) システムの復旧：通信能力を復旧する方法及び手順が，目標復旧時間（RTO／Recovery Time Objective）の点から規定されなければならない。これは，要求される通信リンク及びプロセス機能を復旧 するのに必要な時間と定義される。

2) データの復旧：OT システムの安全な状態及び船舶の安全運航を復元するのに必要なデータを復旧する方法及び手順が，目標復旧時点（RPO／Recovery Point Objective）の点から規定されなければならない。これは，データの欠損が許容される最長の時間と定義される。

iv) 復旧の目標が決まったら，起こりうるサイバーインシデントの一覧が作成され，復旧手順が作成及び記載されなければならない。復旧計画書は，次に掲げる情報を含む又は参照するものでなければならない。

1) 二重化されている，独立した又は機側からの操作を中断することなく，故障したシステムを復元するための指示及び手順

2) 情報のバックアップ及び安全な保存のためのプロセス及び手順

3) 完全かつアップデートされた論理的ネットワーク図

4) 故障したシステムの復元に責任を有する人員の一覧表

5) サポート業者，ネットワーク管理者等を含む，外部の技術サポートに連絡するための，通信手順及び人員の一覧表

6) すべてのコンポーネントに関する現在の設定情報

v) 当該計画書において，船上の人員の安全確保を手助けするために，船舶の運用及び航行が優先されなければならない。

vi) 復旧計画書は，サイバーセキュリティに責任を有する人員及びサイバーインシデントに際して手助けすることを課された人員が，船上及び陸上において紙で利用可能なものでなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，供給者から提供された情報であって，サイバーイン

シデントからの復旧計画を策定する際に船主が適用しうるものへの言及（**4.4.1(8)**参照）を含めなければならない。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，**5.4.6(2)**及び**(3)**に規定するサイバーインシデントに対応するために供給者が提供した手順及び指示の有効性を実証しなければならない。なお，当該要件は，**2.2.3-4.(2)**に規定するコンピュータシステムの認証において実施した場合には省略することができる。

iv) 運用段階

運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

1) 船主は，船舶サイバーセキュリティ・レジリエンス計画書に，インシデント復旧計画について記載しなければならない。当該計画書は，本章の適用範囲内にあるコンピュータシステムを取り扱い，少なくとも本章中の次に掲げる要件に対処するものでなければならない。

－ **5.4.6(1)**に規定する要件に従った，誰が，いつ，どのようにサイバーインシデントから復元及び復旧するかに関する説明。

－ **5.4.6(2)**に規定する要件に従った，バックアップに関するポリシーであって，頻度，許容可能なダウンタイムを考慮したバックアップの保守及び試験，制御のための代替手段の利用可能性，ベンダーによるサポート体制並びにコンピュータシステムの重要性について対処したもの。

－ **5.4.6(2)**及び**5.4.6(3)**に規定する要件に従った，コンピュータシステムのバックアップ，シャットダウン，リセット，復元及び再起動に関するユーザーマニュアル又は手順の参照。

2) 初回の年次検査

船主は，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を証明する記録又はその他の文書化された証拠，すなわち次に掲げるものを，本会に提出しなければならない。

－ インシデントからの復旧のための指示及び／又は手順を，船上における責任者が利用可能であること。

－ 復旧に必要な機器，ツール，文書並びに／又はソフトウェア及びデータを，船上における責任者が利用可能であること。

－ コンピュータシステムのバックアップが，ポリシー及び手順に従って行われていること。

－ シャットダウン，リセット，復元及び再起動に関するマニュアル及び手順を，船上における責任者が利用可能であること。

3) 2 回目以降の年次検査

船主は，本会の要請に応じて，初回の年次検査に規定された記録又はその他の文書化された証拠を提示することにより，船舶サイバーセキュリティ・レジリエンス計画書の内容の実施を実証しなければならない。

(2) バックアップ及び復元の機能

(a) 要件

本章の適用範囲内にあるコンピュータシステム及びネットワークは，時宜にかない完全で安全な方法によるバックアップ及び復元を支える機能を有するものでなければならない。バックアップは定期的に保守及び試験されなければならない。

(b) 根拠

一般に，バックアップ及び復元に関する戦略の目的は，データ喪失からの防御及び当該データ喪失後のデータベース再構築であろう。通常は，バックアップの管理タスクには，次に掲げるものが含まれる。

i) 異なる種類の故障に対する対応の計画及び試験

ii) バックアップ及び復旧のためのデータベース環境の設定

iii) バックアップのスケジュールの決定

iv) バックアップ及び復旧環境の監視

v) 長期保存用のデータベースの写しの作成

vi) データベース間又はホスト間でのデータの移動等

(c) 要件の詳細

i) 復元の機能

1) 本章の適用範囲内にあるコンピュータシステムは，サイバーインシデントの後，船舶が航行及び運用できる状態に安全に復帰可能とするための，バックアップ及び復元の機能を有するものでなければならない。

2) データは，安全なコピー又はイメージから復元可能でなければならない。

3) 情報及びバックアップの設備は，サイバーインシデントから復旧するのに十分なものでなければならない。

ii) バックアップ

1) 本章の適用範囲内にあるコンピュータシステムは及びネットワークは，データのバックアップを提供するものでなければならない。オンラインのバックアップ機器に影響するランサムウェア及びワームに対する許容範囲を改善するために，オフラインのバックアップの使用も考慮されなければならない。

2) バックアップ計画書であって，範囲，モード及び頻度，保存媒体並びに保存期間を含むものが作成されなければならない。

(d) 適合の実証

i) 設計段階

要件なし。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，本章の適用範囲内にあるコンピュータシステムの供給者が提供するバックアップ及び復元の手順及び指示を実証しなければならない。なお，当該要件は，**2.2.3-4.(2)**に規定するコンピュータシステムの認証において実施した場合には省略することができる。

iv) 運用段階

1) 運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

2) 定期検査

コンピュータシステムに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

(3) 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

(a) 要件

i) 本章の適用範囲内にあるコンピュータシステム及びネットワークは，サイバーインシデントにより起こりうる障害から早く安全に復旧できるように，制御されたシャットダウン，初期状態へのリセット，安全な状態へのロールバック及び電源オフからそのような状態での再起動が可能なものでなければならない。

ii) 前 **i)**の操作をどのように実行するかに関する適切な文書が，船上の人員に利用可能でなければならない。

(b) 根拠

i) 制御されたシャットダウンとは，コンピュータシステム又はネットワークの電源を切る際に，接続された他のシステムが実行中の処理を実施／中止し，終了して，接続を切る等を，ソフトウェアの機能により可能にして，統合されたシステム全体を安全で既知の状態におくことである。制御されたシャットダウンは，コンピュータが電源喪失により強制的にシャットダウンされる際等に起こるハードシャットダウンと対照的である。

ii) サイバーインシデントの中にはハードシャットダウンが安全な予防策と考えられるものもあるが，統合されたシステムの場合には，つじつまが合い動作が予測可能である既知の状態に維持するために，制御されたシャットダウンが好ましい。通常のシャットダウン手順が行われない場合には，データ又はプログラム及びオペレーティングシステムファイルの破損が起こりうる。OT システムの場合には，当該破損の結果が，不安定な状態，正しくない機能又は予定されたサービス提供の失敗となりうる。

iii) リセット操作とは，通常は，ソフトブートで始まり，システムにシャットダウンのプロセスを行わせ，メモリを消去して，デバイスを初期状態に戻すことである。システムによっては，リセット操作が異なる影響をもたらすこともある。

iv) ロールバックとは，システムを以前の状態に戻す操作である。間違った操作の実行後であってもシステムのデータ及びプログラムを無傷のコピーに復元可能であるため，ロールバックはデータ及びシステムの完全性に関して重要である。ロールバックは，クラッシュ及びサイバーインシデントから復旧し，つじつまの合う状態に復元するうえで極めて重要である。

v) システムの再起動並びに読取り専用情報源からのすべてのソフトウェア及びデータの再読込み（例えば，ロールバック操作後）は，想定外の不具合又はサイバーインシデントからの復旧に効果的な方法である。ただし，単一のコンポーネントにおける想定外の再起動がシステムの状態の食い違い又は予測不可能な動作をもたらしうることから，特に統合されたシステムにおいて再起動の操作は制限されるべきである。

(c) 要件の詳細

i) 本章の適用範囲内にあるコンピュータシステム及びネットワークは，次に掲げることが可能なものでなければならない。

1) 制御されたシャットダウンにより，接続された他のシステムが実行中の処理を実施／中止し，終了して，接続を切る等ができるようにして，統合されたシステム全体を安全でつじつまの合う既知の状態におくこと。

2) リセットにより，システムにシャットダウンのプロセスを行わせ，メモリを消去して，デバイスを初期状態に戻すこと。

3) システムの完全性及び一貫性を復元すべく，以前の設定及び／又は状態にロールバックすること。

4) 再起動及び読取り専用情報源からのすべてのソフトウェア及びデータの再読込み（例えば，ロールバック操作後）。再起動の時間は，システムの予定されたサービスに合ったものでなければならず，他の接続されたシステム又は統合されたシステムを食い違った又は安全でない状態にするものであってはならない。

ii) システムがサイバーインシデントの影響を受けた場合に，上述の操作をどのように実施するかに関する文書が，船上の人員に利用可能でなければならない。

(d) 適合の実証

i) 設計段階

統合者は，サイバーセキュリティデザインの説明に，本章の適用範囲内にあるコンピュータシステムを安全にシャットダウン，リセット，復元及び再起動する方法を説明する製品説明書又は手順への参照を含めなければならない。

ii) 建造段階

要件なし。

iii) 試運転段階

統合者は，本会に船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を提出し，本章の適用範囲内にあるコンピュータシステムのシャットダウン，リセット及び復元のためのマニュアル又は手順が確立されていることを実証しなければならない。当該マニュアル／手順は，船主に提供されなければならない。なお，当該要件は，**2.2.3-4.(2)**に規定するコンピュータシステムの認証におい実施した場合には省略することができる。

iv) 運用段階

1) 運用段階における検査の一般要件については，**2.2.3-5.**を参照すること。

2) 定期検査

コンピュータシステムに改造が加えられた場合，船主は，船舶サイバーレジリエンス試験要領書に従って，**iii)**に規定する事項を本会に実証しなければならない。

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

5.5.1 要件

本章の適用範囲内にあるコンピュータシステムのいずれかを関連要件の適用対象から除外する場合には，リスク評価が実施されなければならない。リスク評価では，除外されるコンピュータシステムに関連するリスクレベルが許容可能である証拠を提供しなければならない。

5.5.2 根拠

-1. 本章の適用範囲内にあるコンピュータシステムを関連要件の適用対象から除外する場合には，十分に正当であると理由づけられ，文書化されなければならない。当該除外は，コンピュータシステムの運用に関連するリスクレベルが許容可能な閾値を下回るという証拠が，個別のリスク評価によって示された場合にのみ，本会によって受け入れられる。

-2. リスク評価は，コンピュータシステムの分類，接続性並びに船舶及びコンピュータシステムの機能要件及び仕様を考慮して，利用可能な知識ベース及び類似の設計に関する経験（もしある場合）に基づくものでなければならない。内部及び外部の情報源からのサイバー脅威に関する情報は，サイバーセキュリティ事象の発生確率及び影響度に対して理解を深めるために使用することができる。

5.5.3 要件の詳細

-1. リスク評価は，統合者によって，もとの設計に加えられうる変更並びに初めは知られておらず新たに発見される脅威及び／又は脆弱性を考慮して，設計及び建造段階において実施され，最新の状態に保たれなければならない。

-2. 船主は，船舶の運用期間にわたって，サイバーシナリオの絶え間ない変化及び継続的な改善のプロセスにおいて船上のコンピュータシステムに新たに識別される弱点を考慮して，リスク評価をアップデートしなければならない。新たなリスクが識別された場合，船主は，既存のリスク低減策をアップデートするか，又は，新たなリスク低減措置を実装しなければならない。

-3. サイバーシナリオの変化により，検討対象のコンピュータシステムに関連するサイバーリスクが許容可能な閾値を超える場合，船主は，本会に通知し，アップデートされたリスク評価を検証のために提出しなければならない。

-4. 検討対象のコンピュータシステムに想定される運用環境は，サイバーインシデントの発生確率及びそれが人の安全，船舶の安全又は海洋環境に及ぼす影響度を見定めるために，コンピュータシステムの分類も考慮してリスク評価において分析されなければならない。攻撃対象領域は，コンピュータシステムの接続性，考えられる可搬式デバイスのインターフェース，論理的なアクセス制限等を考慮して分析されなければならない。

-5. 検討対象のコンピュータシステムの，特定の構成に関連して生じるリスクについても識別されなければならない。リスク評価においては，次に示す要素が考慮されなければならない。

(1) 資産の脆弱性
(2) 内的及び外的脅威
(3) 資産に影響するサイバーインシデントが，人の安全，船舶の安全及び／又は環境への脅威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して考えられる影響。ここでいうシステムには，（船上のシステムへの遠隔アクセスが提供されている等の場合には）船外にあるものを含む。

5.5.4 合格基準

-1. 本章の適用範囲内にあるコンピュータシステムを関連要件の適用対象から除外することは，当該コンピュータシステムの運用が，サイバーリスクに関して，運用上の安全性に影響を及ぼさないことが確保される場合に限り，本会によって受け入れられる。当該除外は，以下に掲げる追加基準を完全には満たさないコンピュータシステムについても，証拠とともに合理的な説明が提供され，本会が適当と認める場合には，受け入れられることがある。また，本会は，当該除外を検討するために追加書類の提出を求めることがある。

-2. システムを本章の適用範囲から除外するためには，以下に掲げる基準が満たされなければならない。

(1) コンピュータシステムは隔離されていなければならない。（すなわち，他のシステム又はネットワークへの IP ネットワーク接続がない）
(2) コンピュータシステムはアクセス可能な物理的なインターフェースのポートを持たないものでなければならない。使用されていないインターフェースは論理的に使用できない状態にしなければならない。許可されていないデバイスを当該コンピュータシステムに接続することは不可能でなければならない。
(3) コンピュータシステムは，物理的アクセス制御が実装されている場所に配置されなければならない。
(4) コンピュータシステムは，本章の適用範囲内にある船舶の機能のうち複数のものを提供する，統合された制御シス

テムであってはならない。

-3. リスクレベルの許容性を評価する際には，以下の追加基準が考慮されるべきである。

(1) コンピュータシステムは，分類 III に該当する船舶の機能を提供するものでないこと。

(2) 既知の脆弱性，脅威，コンピュータシステムに影響するサイバーインシデントから派生する潜在的な影響が，リスク評価において適切に考慮されること。

(3) コンピュータシステムの攻撃対象領域が，その複雑さ，接続性，物理的及び論理的なアクセスポイント（無線アクセスポイントを含む）を考慮して，最小化されること。

目次

鋼船規則検査要領 X 編　コンピュータシステム

X3　　コンピュータシステム

X3.2　　システム及びコンポーネントの承認

X3.2.1　　システムの承認

規則 X 編 3.2.1-2.にいう「本会が別に定めるところ」とは，**事業所承認規則**に基づく審査の際に，次に掲げる事項についても確認することをいう。

(1) 対象のコンピュータシステムが，**規則 X 編 3.2.2** にいう使用承認（**規則 X 編 2.2.1-1.**にいう品質計画書及び品質マニュアルについての確認を含む）を受けたものでなければならない。なお，使用承認を受けるための試験等は，**事業所承認規則**に基づく審査と同じ時期に実施しても差し支えない。

(2) 対象の製造事業所が，**規則 X 編 2.2.1-1.**にいう品質計画書及び品質マニュアルに基づき，品質管理システムを履行していること。

X3.3　　システムの分類

X3.3.3　　システムの分類の例

規則 X 編 3.3.3(1)(c)にいう「診断及びトラブルシューティングシステム」に，**検査要領 B 編 B9.1.4-5.(2)**に規定する状態監視システムは該当しない。

X3.4　　コンピュータシステムの開発及び承認に関する要件

X3.4.2　　システム供給者の要件

-1. **規則 X 編 3.4.2-3.**にいう「システムの仕様書及び設計書」とは，同 **3.4.2-3.(2)(a)**から**(h)**に掲げる内容を含む資料をいい，複数の文章等にその記載内容を分割しても差し支えない。

-2. **規則 X 編 3.4.2-5.**にいう「品質保証活動」で利用される手法の中には，「単体（ユニット）テスト」又は「デベロッパーテスト」と呼ばれるものもあり，コードレビューや静的又は動的プログラム解析等の確認手法も含まれる場合がある。

-3. **規則 X 編 3.4.2-7.**にいう「船舶に搭載する前の FAT」とは，本章の規定に従ってコンピュータシステムに対して実施される試験のみをいい，他の編に規定する「製造工場等における試験」とは別に追加で実施するものである。また，複雑なシステムの場合，「FAT 前にシステム供給者が行うシステム試験」と FAT の範囲が大きく異なる場合がある一方で，一部のシステムおいては同一となることがある。

X3.4.3　　統合者に関する要件

-1. **規則 X 編 3.4.3-4.**において，リスク評価の方法を決定するために，*IEC/ISO* 31010 “Risk management—Risk assessment techniques”を参照にすることができる。

-2. **規則 X 編 3.4.3-6.**に規定する SAT 及び同**-7.**に規定する SOST の内容は，システムが複雑である場合には大きく異なることがある。一方で，両者の内容が重複する又は同一となるシステムもある。このため，SAT 及び SOST の内容が類似している場合には，本会は，SAT が SOST を兼ねるものとし，試験方案及び試験報告書についてもそれぞれ共通のものとすることを認めることがある。

X3.6 変更管理

X3.6.3 ステークホルダー間の合意

規則 X 編 3.6.3 において，一般に，変更管理は少なくとも次の**(1)**から**(3)**に示す段階を扱う。

(1) 開発から FAT 前にシステム供給者が行うシステム試験まで
システム供給者及び当該システム供給者への供給者が関係する。

(2) FAT から所有者への船舶引渡しまで
システム供給者，統合者，所有者及び本会が関係する。

(3) 就航後
システム供給者，サービス提供者，所有者及び本会が関係する。

X4　船上のシステム及び機器のサイバーレジリエンス

X4.1　一般

X4.1.1　通則

-1. 船舶，港，コンテナターミナル等の技術的進化並びに運用技術（OT）及び情報技術（IT）への依存の高まりにより，ビジネス，人事情報，人の安全，船舶の安全に影響を与え，また，海洋環境への脅威となり得るサイバー攻撃が増加する可能性が高まっている。現在及び将来の脅威から海運を保護するには，機器及びシステムの設計及び製造段階におけるセキュリティ機能の組込みを要するような，継続的に発展する一連の管理策を含める必要がある。従って，サイバーレジリエントといえるシステム及び機器を提供するための，共通の最低要件を制定することが必要である。

-2. コンピュータシステム及びサイバーレジリエンスに関する，次に示す要件にも注意しなければならない。

(1) **規則 X 編 3 章**「コンピュータシステム」

(2) **規則 X 編 5 章**「船舶のサイバーレジリエンス」

(3) *IACS* Recommendation No.166「Recommendation on Cyber Resilience」（*IACS* Recommendation No.166 は，サイバーレジリエントな船舶であって，そのレジリエンスを一生にわたって維持することが可能であるものの建造を支援するために，利害関係者が参照及び適用することができる，推奨される非強制の技術要件である。）

X4.4　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

X4.4.2　要求されるセキュリティ機能

-1. **規則 X 編表 X4.1** 中 **10** の適用上，ポートの制限／ブロッカー（及びシリコン）は，特定のシステムでは受け入れられうる。

-2. **規則 X 編表 X4.1** 中 **17** の適用上，無線ネットワークに暗号化の仕組みを採用すること。

-3. **規則 X 編表 X4.1** 中 **21** の適用上，無線ネットワークの場合，伝送中のすべての情報の機密性を保護するために，暗号化の仕組みを採用すること。

-4. **規則 X 編表 X4.1** 中 **24** の適用上，DoS イベント発生中に，コンピュータシステムが縮退運転することは許容されるが，危険な状況を引き起こす可能性のある方法で故障しないこと。過負荷ベースの DoS イベント，すなわちネットワーク容量のフラッド攻撃が試みられ，コンピュータのリソースが消費されようとするような場合を考慮すべきである。

X5　船舶のサイバーレジリエンス

X5.1　一般

X5.1.1　目的

-1. 船上におけるコンピュータシステムの相互接続により，船上における商用オフザシェルフ（COTS）の製品の利用が広まるのとあいまって，人事情報，人の安全及び船舶の安全に影響を与え，また，海洋環境への脅威となるような攻撃の可能性が高まっている。船内システムと外部世界との間にネットワーク接続又はその他のインターフェースがある場合，攻撃者はその目的を達成するために人及び技術のあらゆる組み合わせを標的としうる。船舶及び海運全般を現在及び将来の脅威から保護するには，継続的に発展する様々な対策がある。このため，実際にサイバーレジリエントといえる船舶を提供するために，共通である最低限の機能及び性能基準を制定することが必要である。IACS は，サイバーレジリエントな船舶を実現するためには，ゴールベースのアプローチを用いた，脅威全体に対して一貫して適用される最低限の要件が必要であると考える。

-2. **規則 X 編 5 章**の構成は，**表 X5.1.1-1.**のとおりとする。

表 X5.1.1-1.　**規則 X 編 5 章**の構成

導入部	5.1　一般
	5.2　定義
	5.3　目的及び要件の構成
主要部	5.4　船舶のサイバーレジリエンスの要件 5.4.1　一般 5.4.2　識別 5.4.3　防御 5.4.4　検知 5.4.5　対応 5.4.6　復旧
補足部	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（システムが**規則 X 編 5 章**の適用対象から除外される場合にのみ要求される）

X5.2　定義

X5.2.1　用語

規則 X 編 5.2.1(13)にいう「ネットワークセグメント」において，ネットワークアドレスプランの先頭部分には IP アドレス及びネットワークマスクが付く。ネットワークセグメント間の通信は，ネットワーク層（OSI 参照モデルの第 3 層）におけるルーティング機能を使用した場合に限って可能である。

X5.4　船舶のサイバーレジリエンスの要件

X5.4.3　防御

規則 X 編 5.4.3(4)(c)v)において，コンピュータシステムは，**規則 X 編表 X4.1** 中 **1** に従って，ユーザー（人）を識別及び認証しなければならない。つまり，すべてのユーザー（人）を「一意に」識別し，認証する必要はない。