CHARTING THE FUTURE

ClassNK

船舶のサイバーレジリエンスに関するガイドライン

（第 1.0 版）

［日本語 / Japanese］

Cyber Resilience of SHIPS

Copyright @ 2024 Nippon Kaiji Kyokai
禁無断転載

改訂履歴

No.	日付	区分	改訂内容
1.0	2024.07.12	新規	新規作成

ClassNK

はじめに

従来の舶用システムは物理的な接続や制御に依存しており、サイバー攻撃等の脅威は想定されていませんでした。しかし、近年これらがコンピュータやインターネットを介してデジタル的に相互接続されるようになりました。これにより、舶用システムはサイバー空間にさらされるようになり、サイバー攻撃のリスクが高まり、一部の船舶では実害も発生しています。このような背景からサイバーセキュリティが注目されることとなりました。

2022 年 4 月、IACS（International Association of Classification Societies：国際船級協会連合）によって、サイバーセキュリティに関する 2 つの UR（Unified Requirement：統一規則）が新規に発行されました。それが、UR E26 及び UR E27 です。これらは、サイバー攻撃等によるサイバーインシデントの発生を低減し、影響を軽減し、発生した場合でも早期に復旧する機能（以下、サイバーレジリエンス）に関する要件であり、UR E26 では船舶が、UR E27 では船上のシステム及び機器が対象として定められております。これらの目的は、サイバーレジリエンスに関する最低限の要件を船舶、船上のシステム及び機器に適用することで、サイバーセキュリティを最低限確保した船舶を実現することにあります。UR E26 及び E27 の発行を受けて、日本海事協会（以下、本会）では、これらの要件を鋼船規則 X 編（以下、X 編）に取り入れることとしました。

今回初めてサイバーセキュリティ対策が新造船への強制要件として取り入れられることになったことを受けて、本会では関係者に理解を深めていただく一助として、本ガイドラインを発行することと致しました。

本ガイドラインは、X 編 5 章（UR E26）の解説本となります。主に、統合者（主に造船所）及び船主（又は船舶管理会社）を対象としております。具体的には、以下の事項について解説する手引きとなっています。

・適用範囲及び承認プロセス

船舶及びシステムの適用範囲を含め、本会の承認を取得するための手順を解説しております。

・提出資料及び立会検査の要件

船舶に対するサイバーレジリエンスの要件について、提出資料及び立会検査の詳細をそれぞれの項目ごとに解説しております。

本ガイドラインにはサイバーセキュリティに関する専門性の高い内容が含まれますが、X 編 5 章（UR E26）の全容を掴んでいただくために、「1 章 概要」にわかりやすく基本情報と全体像をまとめております。

本ガイドラインの構成

本ガイドラインは、以下の利害関係者を対象としています。

- 統合者：セキュリティ設計及びネットワーク構築の担当者を指す。特に契約／指定される場合を除き、造船所となる。
- 船主：船主又は船舶管理会社を指す。

---

1 章　概要

X 編 5 章（UR E26）の全体像について解説します。X 編 5 章（UR E26）では、全体の目的である「サイバーレジリエンスを確保した船舶を建造すること」を達成するために、その目的を 5 つの機能要素に分解した上で、それぞれの要件を設定しております。本章では、5 つの機能要素（識別、防御、検知、対応、復旧）について、その目的及び内容をより理解しやすいよう解説しております。本章により、それぞれの目的及び内容を把握することで、X 編 5 章（UR E26）全体の目的を掴み、船舶が達成すべきゴールを明確にします。

- 統合者及び船主：X 編 5 章（UR E26）の全体像を把握する。

2 章　適用

X 編 5 章（UR E26）の適用範囲について解説します。X 編 5 章（UR E26）では、船舶及びシステムの適用範囲が定められております。本章では、X 編 5 章（UR E26）が適用される船舶及びシステムがより明確に把握できるよう、具体例を示しております。ネットワークの設計に従って、X 編 5 章（UR E26）におけるシステム及びネットワークの適用範囲が決定されます。そのために、システムの適用範囲を正しく把握するための一例を提供します。

- 統合者：船舶及びシステムの適用範囲を把握することで、ネットワーク及びセキュリティの設計を支援するための情報を入手する。
- 船主：X 編 5 章（UR E26）について、どのような船舶及びシステムが適用となるかを理解する。特に、自らが支給する可能性のある IT 機器（ECDIS や VDR に使用されるサーバー等。詳細は本ガイドライン 2-2.2 参照）が X 編 5 章（UR E26）にどのように関わるかを把握する。

3 章　適合のためのプロセス

X 編 5 章（UR E26）のプロセスについて解説します。X 編 5 章（UR E26）では、利害関係者として供給者・統合者・船主及び本会を挙げており、4 つの段階（設計段階、建造段階、試運転段階及び運用段階）にて各利害関係者への対応を求めております。本章では、それぞれの段階（設計段階、建造段階、試運転段階及び運用段階）に対する統合者及び船主が取るべき行動を、作成すべき図書等をベースに示します。本章により、X 編 5 章（UR E26）のプロセスにおいて、求められる提出資料及び立会検査の一覧を把握するための情報を提供します。

- 統合者：各段階（特に、設計段階、建造段階、試運転段階）における提出資料及び立会検査を明確にし、取るべき行動を把握する。
- 船主：各段階（特に、運用段階）における提出資料及び立会検査を明確にし、取るべき行動を把握する。

4 章　提出資料の解説

X 編 5 章（UR E26）の提出資料について解説します。統合者は建造中登録検査時に、船主は初回の年次検査までに該当する資料の提出が求められています。本章では、提出資料の詳細を解説します。

- 統合者：各段階（特に、設計段階、建造段階、試運転段階）における提出資料の詳細を把握する。
- 船主：運用段階における提出資料の詳細を把握する。

5 章　立会検査の解説

X 編 5 章（UR E26）の立会検査について解説します。統合者は試運転段階において、船主は定期的検査時に該当する検査の実施が求められています。本章では、立会検査の詳細を解説します。

- 統合者：試運転段階における立会検査の詳細を把握する。
- 船主：定期的検査における立会検査の詳細を把握する。

目次

1 章　概要 1
2 章　適用 7
2-1. X 編 5 章（UR E26）が適用される船舶 7
2-2. X 編 5 章（UR E26）が適用されるシステム 7
2-2.1 船上の運用技術（OT）システム 7
2-2.2 OT システムと IT システムの両方に接続されるシステム 10
2-2.3 X 編 5 章（UR E26）の適用対象であるネットワークとそれ以外のネットワーク間の通信インターフェース 14
3 章　適合のためのプロセス 16
3-1. 設計・建造段階 16
3-2. 試運転段階 19
3-3. 運用段階 20
4 章　提出資料の解説 22
4-1. 船舶資産インベントリ 23
4-1.1 概要 23
4-1.2 解説 23
4-2. ゾーン及びコンジット図 27
4-2.1 概要 27
4-2.2 解説 27
4-3. サイバーセキュリティデザインの説明 32
4-3.1 概要 32
4-3.2 解説 32
4-3.3 機能要素毎の各要件の解説 32
4-4. 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 49
4-4.1 概要 49
4-4.2 解説 49
4-5. 補完的対策の説明 52
4-5.1 概要 52
4-5.2 解説 52
4-6. 船舶サイバーレジリエンス試験要領書 54
4-6.1 概要 54
4-6.2 解説 54
4-6.3 機能要素毎の各要件の解説 55
4-7. 船舶サイバーセキュリティ・レジリエンス計画書 76
4-7.1 概要 76
4-7.2 解説 76
4-7.3 機能要素毎の各要件の解説 77
5 章　立会検査の解説 104
5-1. 試運転段階での検査 105
5-2. 初回の年次検査 108

5-3. 2 回目以降の年次検査／中間検査 110
5-4. 定期検査 111

ClassNK

1章　概要

この章では、X 編 5 章（UR E26）の全容を把握するためにその全体像を解説します。

X 編 5 章（UR E26）は、船舶のサイバーレジリエンスに関する要件です。サイバーレジリエンスとは、サイバー攻撃等による人や船舶の安全及び環境に対する脅威につながる船舶の運用技術（OT）の障害の発生を低減し、影響を軽減し、発生した場合でも早期に復旧する機能です。船舶に対してこのような機能を実装し、サイバー攻撃等に耐性をもった船舶とすることが、X 編 5 章（UR E26）の狙いです。

船舶にサイバーレジリエンスを確保するために、X 編 5 章（UR E26）では、5 つの機能要素（識別、防御、検知、対応、復旧）に分解した上で、それぞれの要件を設定しております。

図 1.1　X 編 5 章（UR E26）の概念図

識別

「識別」の主目的は、船舶が所有するシステムやネットワーク機器などの資産を「見える化」することです。具体的には、船舶の資産に関するインベントリ（台帳）を作成することになります。このインベントリは船舶資産インベントリと呼ばれ、船舶に今現在どのようなコンピュータシステム及び機器が搭載されているかを明確にします。

図 1.2 船舶資産インベントリ

船舶資産インベントリは、メーカーが供給した製品の OS、ソフトウェア等の製品情報を集め、さらに本船のネットワークとして組み上げた後の搭載場所及び接続されている機器、外部からのアクセスの有無などを含めた台帳としてまとめたものです。

船舶資産インベントリを最新情報に維持することで、資産を把握しやすくなり、以下のような効果があります。

- メーカー等から入手した船舶資産に関するセキュリティ上の弱点及びそれを修正するための情報を、船舶資産インベントリの情報と照らし合わせることで、船舶資産のセキュリティリスクを把握することが可能です。
- 船舶資産に関する詳細な情報をあらかじめ見える化することで、セキュリティインシデント発生時に迅速に対応することが可能です。

実際の作業

- 統合者は、システムの OS やソフトウェア等の製品情報を取りまとめ、リスト化することが求められます。
- 船主は、本リストを維持し、必要に応じて更新することが求められます。

防御

「防御」の主目的は、起こりうるサイバーインシデントの規模と頻度を最小化することです。そのために必要となる防護策の実装に関する要件が定められています。本要件で特に重要な点は、船舶の資産と接続されるネットワークを「セグメント化」することです。セグメント化とはネットワークの設計において、コンピュータシステムを用途や重要度にあわせて区画分けすることを指します。

また、同一セグメント内の各機器に対しても必要なセキュリティ対策（不要な機能及びサービスを無効化し、不可欠な機能のみを備える等）を実装することも要求されています。このような設計にすることによって、サイバー攻撃等の被害を受ける可能性を低くし、システムへの影響を抑えることができます。

図 1.3 本要件で求められる特に重要な防護策

上記の防護策を実装することで、以下の効果があります。

- 各機器のセキュリティ対策によって、船舶がサイバー攻撃等による影響を受けるリスクを最小化します。
- ネットワークをセグメント化することで、サイバー攻撃等の影響を受けた場合にその伝搬を防ぎ、被害を最小限に抑えることができます。

実際の作業

- 統合者は、本船のネットワークを設計し、本船に搭載されたコンピュータシステムは不要な機能を無効化する等、正しく設定することが求められます。
- 船主は、実装された防護策を維持するためにシステムと記録の管理が求められます。

検知

「検知」の主目的は、攻撃を特定することです。具体的には、ネットワーク動作の監視を行うとともに、本船に搭載されたセキュリティ機能の有効性を確保することです。平常時には定期的な機能検証を実施し、異常時には警報を発することで、船舶が受けたサイバー攻撃等を早期に認知することができます。

- **ネットワーク動作の監視：**多くのサイバー攻撃には、攻撃中やその前後にネットワーク動作（通信量の増加、通信相手の変更など）が含まれます。これらのネットワークに関する動作を記録すること、攻撃が疑われるような設計範囲外のネットワーク動作で警報を発することにより、攻撃を特定できます。

図 1.4 設計範囲外のネットワーク動作による警報

また、平常時には、上記のネットワーク動作の監視を含めた識別～復旧に関わるシステムに備わったセキュリティ機能が正常に動作していることを検証手順や方法、時期を策定したうえで検証する必要があります。それにより船舶のサイバー攻撃等への耐性が高まります。

図 1.5 定期的なセキュリティ機能の検証による保護

実際の作業

- 統合者は、ネットワーク動作の監視機能及びセキュリティ機能の検証方法を取りまとめることが求められます。
- 船主は、ネットワーク動作の監視機能の利用手順の文書化、セキュリティ機能の有効性の検証が求められます。

対応

「対応」の主目的は，検知されたサイバーインシデントの影響を最小化するための手段を検討し実践することです。具体的には、インシデントにどのように対応するかを規定したインシデント対応計画書を作成し、それに従って行動することが求められます。

当該計画書には以下の情報を含める必要があります。

- **機側，独立及び／又は手動の操作：**サイバーインシデント発生時に、主機及び可変ピッチプロペラ等の推進装置に対して要求される機側又は手動制御を誰がどのように実施するかに関する具体的な手順です。
- **ネットワークの隔離：**サイバーインシデント発生時に，ネットワーク隔離する場合に、誰がどのように実施するかに関する具体的な手順です。
- **ミニマルリスクコンディションへのフォールバック：**「ミニマルリスクコンディションへのフォールバック」とは，サイバーインシデント発生時の，生じうる安全上のリスクを減らすための安定的な停止状態を意味します。本計画書では，統合者が提供するコンピュータシステム毎の情報を参照し、サイバーインシデント発生時にいかにして安定的な停止状態に達するかに関する具体的な手順を作成する必要があります。

図 1.6　インシデント対応計画書

インシデント対応計画書を作成することで、サイバーインシデント発生時に，船上における責任者が各人員に指示を出し，各人員がそれぞれの役割を迅速かつ正確に果たすことができます。その結果、被害を最小限にとどめることができます。

実際の作業

- 統合者は、船主がインシデント対応計画書を作成するための情報をまとめ、文書化することが求められます。
- 船主は、インシデント対応計画書を作成し，インシデント発生時には当該計画書に従って責任者が指示を出し，各人員がそれぞれの役割を迅速かつ正確に果たすことが求められます。

復旧

「復旧」の主目的は、サイバーインシデントによる混乱又は故障の後、使用可能な状態へ回復することです。本要件に従った復旧計画を立案・実施することで、コンピュータシステム及びネットワークを迅速に回復させます。

復旧計画では、「サイバーインシデントからの復旧における人員の役割と手順」、「保守及び試験を含むバックアップの管理」を、船主のポリシーに基づき立案される必要があります。また、各コンピュータシステムの復旧計画の作成にあたっては、供給者から提供される「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」を参照する必要があります。

図 1.7　復旧計画書

復旧計画書を作成することで、以下のような効果があります：

- インシデントからの復旧のために、各人員がやるべきことが明確になります。
- 各コンピュータシステムに適した手順で復旧ができるようになります。

実際の作業

統合者は、各コンピュータシステムの復旧手順等、船主が復旧計画書を作成するための情報をまとめ、文書化することが求められます。

船主は、保守及び試験を含むバックアップの管理を行うこと、復旧時には、本計画手順に従って迅速かつ正確な作業が求められます。

2章　適用

この章では、X 編 5 章（UR E26）の適用範囲について解説します。 X 編 5 章（UR E26）の適用範囲は、以下のとおり決定されます。そのポイントは、ネットワークをどのように構成するかです。特に検討が必要となるのは、OT システムと IT システムの両方に接続するシステムから OT システムをネットワーク設計によってどのように守るかであり、この点については、**2-2.2** で詳しく解説します。

図 2.1　X 編 5 章（UR E26）の適用範囲

2-1. X 編 5 章（UR E26）が適用される船舶

X 編 5 章（UR E26）は、本会に登録する 2024 年 7 月 1 日以降に建造契約が行われる以下の船舶に対して適用となります。

- 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）
- 国際航海に従事する総トン数 500 トン以上の貨物船
- 国際航海に従事する総トン数 500 トン以上の高速船
- 総トン数 500 トン以上の海底資源掘削船
- 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）

2-2. X 編 5 章（UR E26）が適用されるシステム

2-2.1 船上の運用技術（OT）システム

船舶に搭載される運用技術（OT）システムが適用対象となります。運用技術（OT）システムとは、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のことです。*物理プロセス：圧力や温度などの物理的な現象を利用して、作業や変換を行う一連の操作

すなわち、船上の運用技術（OT）システムは、本船の操船、推進、発電、安全等を制御又は監視を行うシステムを指しており、侵害された場合に安全上の懸念が生じる可能性があります。その上で、これらのシステムは、X 編 4 章（UR E27）に従った承認が要求されます。

以下に、適用範囲に含まれると考えられるシステムの例を示します。なお、以下は一例にすぎず、X 編 5 章（UR E26）の適用を決定づけるものではございませんので、その点はご留意ください。

推進

機関制御装置	機関遠隔制御装置
主ボイラ制御装置	CPP 制御装置
電気推進制御装置	燃料供給システム制御装置（例: FGSS 制御装置）
機関警報監視装置（データロガー含む）	ウォータジェット推進制御装置

操舵

操舵システム制御装置	旋回式推進システム制御装置

投錨及び係留

ウインドラス制御装置	ムアリングウインチ制御装置

発電及び分電

発電機制御装置（パワーマネージメントを含む）	電力変換装置（電気推進船等）
バッテリーマネジメントシステム（リチウムイオン電池により構成される総容量 20kWh 以上のもの）	

火災探知及び消火システム

火災探知器（火災表示／警報装置等）	固定式泡消火装置
固定式炭酸ガス消火装置	固定式甲板泡消火装置
局所消火装置	水噴霧装置
ドライケミカル粉末消火装置	

ビルジ及び**バラストシステム**、**積付計算機**

バラスト水遠隔制御装置	積付計算機

水密性及び**浸水検知**

水密扉動力開閉装置	浸水警報装置

照明（例えば、非常灯、低位置、航海灯等）

非常灯装置	低位置照明装置
航海灯制御装置	

安全が要求されるシステムであって、当該システムの混乱又は機能障害が船舶の運航にリスクをもたらしうるもの（例えば、緊急停止システム、荷役安全システム、圧力容器安全システム及びガス検知システム等）

イナートガス装置	荷役監視制御装置
液化ガス緊急遮断装置	可燃性ガス検知装置
液化ガス再液化装置	補助ボイラ制御装置
GCU 制御装置	ガス燃料タンク監視制御装置

条約により要求される**航海設備**

航海用レーダー	船首方位伝達装置（THD）
電子プロッティング装置（EPA)	船舶自動識別装置（AIS）
自動物標追跡装置（ATA）	航海情報記録装置（VDR）
Target Track (TT)（ARPA）	船首方位制御方式自動操舵装置（HCS）
音響測深機	航跡制御方式自動操舵装置（TCS）
衛星航法装置（GPS）	船舶長距離識別追跡装置（LRIT）
音響受信装置	船橋航海当直警報装置（BNWAS）
船速距離計	電子海図情報表示装置（ECDIS）

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**

一般非常警報装置	船内通信装置
ナブテックス受信機	VHF デジタル選択呼出聴守装置
高機能グループ呼出受信機（EGS 受信機）	デジタル選択呼出装置（DSC）
VHF デジタル選択呼出装置	デジタル選択呼出聴守装置

GMDSS 無線設備

その他

自動船位保持設備

2-2.2 OT システムと IT システムの両方に接続されるシステム

2-2.1 に加えて、現在の船舶には OT システムと IT システムの両方に IP 接続するシステムが搭載されることがあります。例えば、外部ネットワークを介して海図データを取得するために ECDIS にインストールされる電子海図用データサーバーや、VDR やテレグラフロガーから運航データを収集しビジネスネットワーク上のパソコンへ転送するデータサーバーなどが挙げられます。（図 **2.2** 参照）また、システムが衛星通信装置と接続される場合、そのファイアウォールに接続される L3 スイッチやルーター等も適用対象となる可能性があります。

図 2.2　船舶ネットワークの概略図

これらの機器が適用対象となるかは、ネットワークの設計方法によります。ここでは、いくつかの代表的なネットワーク設計例を用いて、これらのシステムが適用範囲に含まれるのか解説します。いかなるネットワーク設計においても **2-2.1** の安全に関わるシステムを守るものでなければなりません。

2-2.2.1 OT システムと IT システムの両方に接続されるシステムがないケース

本ケースは OT システムネットワークと IT システムネットワークの両方に IP 接続するシステムが無いケースです。この場合、適用範囲は **2-2.1** の OT システムのみとなります。ま

た、その代表的なネットワーク構成は以下の通りです。

図 2.3　OT システムと IT システムの両方に接続されるシステムがないケースのネットワーク構成図

・想定される運用

電子海図のアップデートは IT ネットワーク上のパソコン上で取得し、そのデータは USB メモリなどの媒体にコピーして OT ネットワーク上の ECDIS に転送される。

・ネットワーク構成に関する解説

適用範囲となる OT ネットワークと IT ネットワークの間は物理的に完全に分離されているため、図 **2.3** 中の❶のファイアウォール等のセキュリティ機器を導入したネットワーク設計は不要です。ただし、媒体や人を介したサイバーリスクは存在するため、X 編 5 章（UR E26）に基づきアクセス管理や媒体管理を講じていかなければなりません。

2-2.2.2 OT システムと IT システムの両方に接続されるシステムがあるケース

■　OT システムと IT システムの両方に接続されるシステムを OT ゾーン内に含める場合

本ケースは OT システムと IT システムの両方に IP 接続されるシステムを OT ゾーン内に含めるケースです。この場合、当該システムも適用範囲に含まれます。そのため、当該システムは **2-2.1** の OT システムと同じゾーンに搭載され、各機器には同等の対策が求められることから、X 編 4 章（UR E27）にあらかじめ適合している必要があります。

その代表的なネットワーク構成は以下の通りです。

図 2.4　OT システムと IT システムの両方に接続されるシステムを OT ゾーンに含める場合のネットワーク構成図

・想定される運用

電子海図のアップデートは図 **2.4** 中の❷の外部と接続する機能をもった ECDIS 用データサーバーを介して陸上のサーバー（電子海図プロバイダ保有のサーバー等）から配信され、ECDIS に転送される。

VDR 上の運航データは図 **2.4** 中の❸の VDR 用データサーバーを介して、IT ネットワーク上のパソコンや船外のパソコンに転送される。

・ネットワーク構成に関する解説

適用範囲となるネットワークと IT ネットワークの間では通信が行われるため、図 **2.4** 中の❹のファイアウォール等のセキュリティ機器を導入し、物理的に分離されている必要があります。

なお、適用範囲となるセキュリティゾーン内に含まれるすべてのシステムは、X 編 4 章（UR E27）に従って承認されている必要があります。

■　OT システムと IT システムの両方に接続されるシステムを DMZ 内に含める場合

本ケースは、OT システムと IT システムの両方に IP 接続されるシステムを DMZ（DeMilitarized Zone：非武装地帯）に含めるケースです。一般的に、ネットワークの設計における DMZ は、外部のネットワークと内部のネットワークの間に配置されるセキュリティゾーンであり、外部からのアクセスを受け入れ、かつ内部ネットワークへの直接アクセスを

防ぐための領域です。船内ネットワークにおいては、OT システムと IT システムの両方に接続されるシステムを DMZ 内に含めることによって、IT ネットワーク経由で当該システムに対して不正アクセスが発生した場合にも OT システムに対する脅威を低減できます。また、就航後の本船ライフサイクルを通じた様々なネットワーク構成変更にも比較的容易に対応することが出来ます。この場合、DMZ 内のネットワークは OT システムが含まれるゾーンの外に配置されるため、DMZ 内の機器の X 編 4 章（UR E27）への適合は不要です。

また、その代表的なネットワーク構成は以下の通りです。

図 2.5　OT システムと IT システムの両方に接続されるシステムを DMZ ネットワーク内に含める場合のネットワーク構成図

・想定される運用

電子海図のアップデートは図 **2.5** 中の❺の外部と接続する機能をもった船上の ECDIS 用データサーバーを介して、陸上のサーバー（電子海図プロバイダ保有のサーバー等）から配信され、ECDIS に転送される。

VDR 上の運航データは図 **2.5** 中の❻の VDR 用データサーバーを介して、IT ネットワーク上のパソコンや船外のパソコンに転送される。

・ネットワーク構成に関する解説

適用範囲となるネットワークと DMZ ネットワークの間では通信が行われるため、図 **2.5** 中の❼のファイアウォール等のセキュリティ機器を導入し、物理的に分離されている必要があります。このネットワーク構成とすることで、ECDIS 用サーバー及び VDR 用データサーバー等のシステムは、X 編 5 章（UR E26）におけるシステムの適用範囲外となることから、X 編 4 章（UR E27）に従った承認は不要になります。

2-2.2.1 及び **2-2.2.2** で挙げた計 3 通りのネットワーク設計について、利点及び欠点を以下のとおりまとめています。

表 2.1　各ネットワーク設計の利点と欠点の比較表

		利点	欠点
OTシステムとITシステムの両方に接続されるシステムがない		• ITネットワーク経由による侵害されるリスクがない	• **ネットワーク経由でのOTシステムのデータの収集ができない** • 手動でのデータ更新による負担増
OTシステムとITシステムの両方に接続されるシステムがある	OTゾーン内に含める場合	• ネットワーク経由でのOTシステムのデータの収集が可能 • ネットワーク経由でのデータ更新による負担減	• 当該システムを経由した侵害されるリスクの発生が懸念 • **当該システムにX編4章（UR E27）に従った承認が必要**
	DMZ内に含める場合	• ネットワーク経由でのOTデータの収集が可能 • ネットワーク経由でのデータ更新による負担減 • **当該システムがセグメント化されることにより、当該システム経由でのOTシステムへの侵害されるリスクは低減** • **当該システムにX編4章（UR E27）に従った承認は不要**	• ネットワーク構成が複雑になり、設計及び運用の負担増

2-2.3 X 編 5 章（UR E26）の適用対象であるネットワークとそれ以外のネットワーク間の通信インターフェース

2-2.2 により X 編 5 章（UR E26）の適用範囲が決定されますが、適用対象となるネットワークとそれ以外のネットワーク間のインターネットプロトコル（IP）ベースの通信においても、X 編 5 章（UR E26）の適用範囲に含まれ、以下の対策が必要になります。

- 適用対象となるネットワークと接続するネットワーク機器（スイッチやファイアウォール等）が適切な設定となっていること
- ネットワーク機器が適切に管理・保守されていること
- 流れるデータが適切に暗号化されていること

また、ネットワーク機器そのものも、X 編 5 章（UR E26）の適用範囲に設置されていることとなり、X 編 4 章（UR E27)に従った承認が要求されます。

図 2.6　適用対象となる通信及び対策が必要なネットワーク機器

3章　適合のためのプロセス

X 編 5 章（UR E26）のプロセスについて解説します。具体的には、船舶の一生におけるそれぞれの段階ごとに統合者及び船主が取るべき行動を作成すべき図書をベースに示します。

まず、X 編 5 章では、利害関係者として統合者及び船主を挙げております。本ガイドラインでは、統合者及び船主を以下のとおりに定義づけております。

統合者：
セキュリティ設計及びネットワーク構築の担当者を指す。特に契約／指定される場合を除き、**造船所**となる。

船主：
船主又は船舶管理会社を指す。（X 編 5 章では、船主／会社と定義）

表 3.1　各段階における統合者及び船主の取るべき行動

	設計・建造段階	試運転段階	運用段階
統合者	P. 16	P. 19	
船主	P. 19	P. 19	P. 20

3-1. 設計・建造段階

設計・建造段階では、統合者が、コンピュータシステムを含む船舶のネットワークを設計し、それに応じて実際にネットワークを構築することが求められます。統合者は、船舶のネットワークに関連した資料を本会へ提出すること等が要求されます。また、船主は、直接要求される規定はございませんが、船舶のネットワークをあらかじめ統合者と共有しておくことが推奨されます。

統合者

設計・建造段階において、統合者の役割は以下のとおりです。

1)　X 編 5 章（UR E26）の適用範囲に含まれるコンピュータシステムを特定する

統合者はまず、X 編 5 章（UR E26）の適用範囲に含まれるコンピュータシステムを特定することが求められます。この特定には、船舶に必要となるコンピュータシステムをリストアップしたうえで、各コンピュータシステムが X 編 5 章（UR E26）の適用範囲に含まれるかどうかを検討する必要があります。適用範囲について、本ガイドライン 2 章「適用」に詳しく解説しております。

2 章 適用　P. 7

なお、コンピュータシステムを特定するにあたり、他の提出資料に先立って後述する「4-2.ゾーン及びコンジット図」をこの段階で作成することを推奨します。ゾーン及びコンジット図とは、船舶のネットワークのレイアウトを視覚的に表現したものです。本資料を作成することにより、X 編 5 章（UR E26）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機器を正確に特定することが可能となります。なお、X 編 5 章（UR E26）の適用範囲が正確に特定できていない場合、以下のような問題が生じる可能性があります。

- X 編 5 章（UR E26）の適用範囲内であるにも関わらず、X 編 4 章（UR E27）が適用されていないコンピュータシステム又はネットワーク機器が設置される懸念。
- 信頼できないネットワークと接続するコンピュータシステムであるが、X 編 4 章（UR E27）における「追加のセキュリティ機能」が実装されていない懸念。

上記のようなケースによって、コンピュータシステム又はネットワーク機器を再発注する等、手戻りが発生する恐れがありますので、ゾーン及びコンジット図を早めに作成することが重要となります。

また、船主から支給される機器についても、あらかじめ特定する必要があります。当該支給品は、船舶のネットワークに構成され、OT システムと直接接続される場合があります。その場合、これらの支給品が X 編 5 章（UR E26）の範囲内に含まれる可能性があるため、注意が必要です。そのため、統合者は、船主から当該支給品に関する情報を速やかに共有することが重要です。

2)　各供給者からコンピュータシステムの承認図書を調達する

1）で特定したコンピュータシステムは、X 編 4 章（UR E27）が適用されるため、同規則に基づき本会により承認されたコンピュータシステムを搭載する必要があります。統合者は、それらコンピュータシステムの承認図書を供給者から調達することが求められます。X 編 4 章（UR E27）で要求される資料は以下のとおりです。

	コンピュータシステムの承認図書（X 編 4 章（UR E27）参照）
□	コンピュータシステム資産インベントリ
□	トポロジー図

□	セキュリティ機能仕様書
□	セキュリティ機能試験要領書（試験結果含む）
□	セキュリティ構成指針
□	セキュア開発ライフサイクル文書
□	コンピュータシステムの保守・検証手順書
□	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
□	変更管理手順書

なお、本図書を入手した段階で必ず確認すべき事項として、セキュリティ機能仕様書に記載された「補完的対策の説明」が挙げられます。補完的対策とは、コンピュータシステムに要求されるセキュリティ機能が実装できない場合において代替する対策です。コンピュータシステムにより提案される補完的対策の中には、追加のネットワーク機器等が必要となるケースがあります。そのため、このような追加機器の購入の要否をこの段階で特定しておくことを推奨します。

3)　提出が要求される図書を作成、本会機関部へ提出する

設計段階において、統合者はセキュリティ及びネットワークに関する図書を作成し、承認を受ける必要があります。必要となる図書は以下のとおりです。それぞれの図書は、本ガイドライン 4 章「提出資料の解説」に詳しく解説しております。

4-1. 船舶資産インベントリ　P. 23

4-2. ゾーン及びコンジット図　P. 27

4-3. サイバーセキュリティデザインの説明　P. 32

4-4. 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　P. 49

4-5. 補完的対策の説明　P. 52

なお、船主支給品に関して、図面設計時に必要な情報が共有されていないケースが想定されます。その場合、当該支給品に関する情報を「TBD」等で表示したうえで、「試運転段階の検査」までに、必要図書を作成・承認を受けてください。

4)　必要に応じて、承認された図書をアップデートする

建造段階において、設計の修正が発生した場合、3)で承認された図書はアップデートされることが求められております。なお、設計の修正は、統合者の変更管理手順に従って実施い

ただく必要があります。

また、3)で示しているとおり、図面承認時に船主支給品に関する情報を「TBD」としている場合、船主から当該支給品の情報を入手次第、該当図書をアップデートしたうえで、「試運転段階の検査」までに、本会の承認を受けてください。

船主

設計・建造段階において、以下の点について留意いただく必要がございます。

船舶のネットワーク内に構成される機器を統合者と共有する

設計・建造段階において、船主が支給する機器は船舶のネットワークに構成され、OT システムと直接接続される場合があります。これらの支給品が X 編 5 章（UR E26）の範囲内に含まれる可能性があるため、注意が必要です。そのため、船主は、統合者に当該支給品に関する情報を速やかに共有することが重要です。

・船主が支給する機器について

船主支給品は、船舶ネットワーク構築において、船主から提供される機器は、以下のようなものが考えられます。

・ネットワーク機器（スイッチ、ルーター、ファイアウォールなど）

・OT システムと IT システムと両方に接続されるシステム（本ガイドライン 2 章「適用」参照）

2 章 適用　P. 7

従来の船舶建造において、これらの機器は、建造の最終段階（海上試運転後～完工までの期間）に据え付けられることが多く、また設計段階でその情報が統合者に共有されないことが一般的でしたが、今後は設計段階からこれらの機器の情報を統合者に提供することが重要となります。

3-2. 試運転段階

試運転段階では、統合者は、船舶のネットワークを構築した後、コンピュータシステム及びネットワークのセキュリティ機能が正常に作動することを確認するための試験の実施が求められます。

統合者

試運転段階において、統合者の役割は以下のとおりです。

1)　必要に応じて、最新の設計書類を本会機関部へ提出する

設計段階において承認された図書に変更があった場合（上記 3-1.4）参照)、試運転段階での試験に先立って、最新版について本会の承認を受ける必要があります。

2)　「船舶サイバーレジリエンス試験要領書」を作成し、本会機関部へ提出する

試運転段階での試験に先立って、試験環境、試験手順、予想される結果及び合格基準等を示した試験方案（船舶サイバーレジリエンス試験要領書）について本会の承認を受ける必要があります。

4-6. 船舶サイバーレジリエンス試験要領書　P. 54

3)　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，本会の立会検査を実施する

船舶のコンピュータシステム及びネットワークのセキュリティの確認試験として、本会検査員立会いの下、試運転段階での検査を実施することが求められます。本試験は、先に述べた「船舶サイバーレジリエンス試験要領書」に従って実施されます。

5-1. 試運転段階での検査　P. 105

また、本検査は、X 編 5 章（UR E26）の適用範囲内のコンピュータシステム及びネットワークを対象とした実証試験であり、適用範囲内のシステムとして船主支給品が含まれる場合は、当該品も検査対象となる旨、ご留意ください。

3-3. 運用段階

船舶完工後、設計・建造～試運転段階までに作成した資料は船主に手交され、運用段階では、船主が、本船の設計時のセキュリティを維持することが求められます。X 編 5 章（UR E26）への適合維持のためには、船舶の運用期間中、当該資料の変更管理が必要です。この変更管理を適切に行うことで、設計時のセキュリティを船舶の一生を通じて維持することが可能です。そのため、船主は、運用と変更管理を適切に行うための手順を示した文書を作成し、運用する必要があります。

船主

運用段階における船主の役割は以下のとおりです。

1)　「船舶サイバーセキュリティ・レジリエンス計画書」を作成し、本会機関部へ提出する

船主は、統合者から提供された図書の情報を基に、運用及び手順を含む「船舶サイバーセ

キュリティ・レジリエンス計画書」を作成し、本会の承認を受ける必要があります。

4-7. 船舶サイバーセキュリティ・レジリエンス計画書　P. 76

2)　初回の年次検査を実施する

初回の年次検査では、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」に基づく運用状況を確認します。したがって、船主は、本計画書を実際に運用し、**初回の年次検査まで**に記録書等の作成等一連のプロセスを完了する必要があります。「初回の年次検査」については、以下に詳しく解説しております。

5-2. 初回の年次検査　P. 108

3)　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」を運用し、必要に応じて承認図書をアップデートする

運用中、コンピュータシステムのアップデートやネットワークの設定変更等セキュリティ機能への影響を与え得る変更があった場合、計画書に基づいて実施し、記録する必要があります。また、統合者からの資料を含む承認図書が変更される場合は、本会によって再承認を受ける必要があります

4)　定期的検査時に、各検査にて要求される立会検査を実施する

定期的検査時には、検査時期に応じた検査（年次、中間、定期検査）を実施し、X 編 5 章（UR E26）の要件への適合を維持しているかを確認します。

5-3. 2 回目以降の年次検査／中間検査　P. 110

5-4. 定期検査　P. 111

4章　提出資料の解説

本章では、X 編 5 章（UR E26）に規定する提出資料に関する詳細を解説します。

X 編 5 章（UR E26）では、船舶のサイバーレジリエンスに関する資料として、計 7 点の提出資料の要件が規定されております。各資料は以下のとおりです。

提出資料の要件

4-1. 船舶資産インベントリ　P. 23

4-2. ゾーン及びコンジット図　P. 27

4-3. サイバーセキュリティデザインの説明　P. 32

4-4. 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　P. 49

4-5. 補完的対策の説明　P. 52

4-6. サイバーレジリエンス試験要領書　P. 54

4-7. 船舶サイバーセキュリティ・レジリエンス計画書　P. 76

X 編 5 章（UR E26）表 X2.4 では、上記資料以外に「承認された供給者の文書」があります。これは、X 編 4 章（UR E27）に基づきメーカーが本会へ提出し、本会の承認を受ける必要がある資料です。建造段階において、供給者から統合者に提出されることが求められております。詳細は、「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ガイドライン」をご覧ください。

4-1. 船舶資産インベントリ

規則　X 編 表 X2.4 番号 4

統合者：提出、完工まで保守　　船主：保守

4-1.1 概要

船舶資産インベントリは、船舶が所有するコンピュータシステムやネットワーク機器などの資産を一覧化した台帳です。（船舶資産インベントリを作成する目的については、1 章の識別をご参照ください。）

具体的には、X 編 4 章（UR E27）に基づき各供給者から提出されたコンピュータシステム資産インベントリに加え、セキュリティ機器を含むネットワーク機器等の情報を 1 つの表にまとめると船舶資産インベントリを作成することが出来ます。

図 4.1 船舶資産インベントリ

船舶資産インベントリは、ある時点の本船上のコンピュータシステムの情報を一覧で把握することが出来、効率的な変更管理に寄与します。

4-1.2 解説

規則　X 編 2.2.3-3(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。

本資料の要件は、X 編 5.4.2(1)に規定されております。本要件について、関連する要件を含め、以下に解説します。

規則　X 編 5.4.2(1)(c)

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）。

船舶資産インベントリには、下記表の内容を記載する必要があります。

表 4.1　船舶資産インベントリの一例

Security Zone	System Category	System	Detailed Machinery / Systems	Location	Trusted network connected to	Untrusted network connected to	IP address / Port No.	Hardware	Software	Updated Log
								. . .	. . .	
(1)				(2)				(3)		(1)

船舶資産インベントリに記載する事項には、主に次の 2 つに大別されます：

(1)　船舶ネットワークにおけるシステムの情報（システムの分類、搭載されるセキュリティゾーン等)（表 4.2 参照）

(2)　システムの位置及び接続先に関する情報（表.4.3 参照）

(3)　システムのハードウェア及びソフトウェアに関する情報（表 4.4 参照）

まず、船舶に搭載する予定のコンピュータシステムについて、「Security Zone（搭載されるゾーン）」、「System Category（システムの分類）*」、「System（システムの名称）」、「Detailed Machinery / Systems（システムの詳細）」を記載し、リスト化します。

* X 編 3 章（UR E22）に基づき統合者が決定する、コンピュータシステムの故障の影響度合いに応じた分類です。

表 4.2　(1) 船舶ネットワークにおけるシステムの情報の一例

Security Zone	System Category	System	Detailed Machinery / Systems		Updated Log
Main propulsion Zone	III	Main propulsion systems	Main engine control system		
			Main engine remote control system (This includes remote control system for turbine system)		
			Main boiler control system		
			CPP control system		
			Electric propulsion control system		
Steering Zone		Steering system control systems	Steering system, Azimuth thruster control system (Only for steering gear control part)		

また、当該インベントリをシステムの位置及び接続先に関する情報を含めていただくことを推奨します。これらの記載をインベントリへ含める要件自体はございませんが、船舶資産の情報を管理する上で、有用となります。なお、これらの情報は機密情報に該当するため、閲覧者を船上の管理者に限定する等、慎重な管理が求められます。

表 4.3　（2）システムの位置及び接続先に関する情報の一例

Location	Trusted network connected to	Untrusted network connected to	IP address / Port No.
Nav. Bri. Deck	VDR	Shore	XXX

X 編 4 章（UR E27）に基づく承認を取得している機器に関しては、表 4.1 中(3)の情報は基本的に供給者から提供される「コンピュータシステム資産インベントリ」に記載されています。したがって、同情報を船舶資産インベントリに反映し、必要に応じて同資料を参照させることが統合者の実際の作業となります。

表 4.4　(3) システムのハードウェア及びソフトウェアに関する情報の一例

Detailed Machinery/ Systems	Hardware							Software					
	Name	Brand/ manufacturer	Model/ type	Short description of functionality/ Purpose	Unique identifier (Cat. II / III)	Physical interfaces	Supported communication protocols	Brand/ manufacturer	Model/ type	Short description of functionality/ Purpose	Version of Software	OS Patch Level	Firmware Patch Level
XXX	Main Unit	XXX	XXX	To ~~~	XXXXX	LAN (2) USB (4) Serial (1)	TCP/IP	XXX	XXX	XXX	XXX	XXX	XXX
	HMI												
	Ethernet switch												
	Main control panel												
	...												

規則　X 編 5.4.2(1)(d)i)2)

船舶資産インベントリには，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まなければならない。また，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，当該インベントリに含まれなければならない

統合者において、追加で搭載したネットワーク機器（スイッチ、ファイアウォール、ルータ等）やセキュリティ機器（IDS や SIEM 等）については、統合者において上記(1)及び(2)の情報を記載します。

また、設計段階において本項で要求される情報が不明な資産（例：船主が支給するデータサーバー等）については、統合者は、表 4.2 に示す情報（「Security Zone（搭載されるゾーン）」、「System Category（システムの分類）」、「System（システムの名称）」、「Detailed Machinery / Systems（システムの詳細）」）を船主から聞き取りのうえ船舶資産インベントリに記載し、その他の情報は可能な限り記載します。初回作成時に記載できなかった項目においては、当該項目を「TBD」とし、情報を入手次第アップデートしてください。本資料は、試運転段階での検査までには最終化される必要があります。

いずれの場合においても、船舶のライフサイクルを通じて船舶資産インベントリは更新・維持されなければならないことを考慮して作成する必要があります。なお、資産インベントリの管理を手動で行う場合、更新作業が煩雑になる可能性があります。そのため、資産インベントリの更新を効率化し、精度を高めるために、システム化が推奨されます。セキュリティ業界では、資産インベントリ管理のシステム化が将来的な慣例となる予定です。

4-2. ゾーン及びコンジット図

規則　X 編 表 X2.4 番号 2

統合者：提出、完工まで保守　　船主：保守

4-2.1 概要

ゾーン及びコンジット図は、X 編 5 章（UR E26）の適用範囲内のシステムとそれ以外のシステムが本船上のネットワークを構築する際にどのようにグループ化され、また異なるグループ間の通信をどのように制御しているかに関する物理的及び論理的情報を図示したものです。

本資料は、本船上のネットワークにつき同一のゾーンに含めるシステムを識別し、ゾーン間の通信について E26 で要求される物理あるいは論理分離の対策がとられているか（ファイアウォール、V-LAN 等）を記載することで作成できます。

本資料は、本船のネットワークがどのように構成されているかを簡単に把握することが出来るため、就航後のメンテナンスを効率的に行うことができます。

4-2.2 解説

規則　X 編 2.2.3-3(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。

本資料の要件は、X 編 5.4.3(1)(d)i)に規定されております。本要件について、関連する要件を含め、以下に解説します。

規則　X 編 5.4.3(1)(d)i)2)

ゾーン及びコンジット図にあっては，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，次の情報を含めなければならない。

- 明確なセキュリティゾーンの表示。
- 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された図解，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。
- 供給者によって納入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図。

- 異なる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（コンジット）図。
- セキュリティゾーン及び信頼できないネットワーク内のシステム間の通信（コンジット）図。

上記要件を解説するサンプル図は以下のとおりです。

図 4.2　ゾーン及びコンジット図のサンプル図

本要件において、重要な点を以下に示します。

・明確なセキュリティゾーンの表示

X 編 5 章（UR E26）の適用範囲を明確にするために、適用範囲内のセキュリティゾーン及び適用範囲外のセキュリティゾーンを明確に区別し示す必要があります。図 4.2 では、適用範囲内のゾーンを実線にて、適用範囲外のゾーンを点線にて示しておりますが、分かりやすく記載することが求められます。

・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

X 編 4 章（UR E27）の承認を受けたコンピュータシステムに関して、供給者から当該システムのトポロジー図が提供されます。ゾーン及びコンジット図では、各コンピュータシステムのトポロジー図を参照できるような記載（トポロジー図への参照リストを作成する、又は図面名称等を明記する等）とすることが求められます。

また、ゾーン及びコンジット図は、以下の要件についても満足するように作成される必要があります。

規則　X 編 5.4.3(1)(c)

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ものとしなければならない。

v)　無線機器は，専用のセキュリティゾーンに含めなければならない。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，これらのシステムがセキュリティゾーンに求められるものと同様の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分離することが可能でなければならない。（5.4.5(3)参照）

上記要件を解説するサンプル図は以下のとおりです。

図 4.3　ゾーン及びコンジット図のサンプル図

本要件において、重要な点を以下に示します。

・セキュリティゾーン内に搭載されるコンピュータシステム及びネットワーク

図 **4.3** 中の i)のセキュリティゾーンに含めるコンピュータシステム及び OT システムと IT システムの両方に接続されるシステムは、**2-2.2.2** で示す通りあらかじめ X 編 4 章（UR E27）に従った承認を受けている必要があります。

・論理的及び物理的なネットワークのセグメント化

図 **4.3** 中の ii), iii)及び vi)の「物理的な分離（Physical segmentation）」及び「論理的な分離化（Logical segmentation）」に関して、下記にその概要図を示します。

図 4.4　物理的な分離及び論理的な分離の概要図

X 編 5 章（UR E26）で要求されるネットワークの論理的及び物理的セグメント化の理解には、まずネットワークセグメントがどのような単位で定義されているか確認することが役立ちます。1 つのネットワークセグメントとは、同一ブロードキャストドメインと定義されており、したがって 1 台の L2 スイッチ（または、カスケード接続*された複数の L2 スイッチ）に接続された機器から構成され、接続されたすべての機器が通信できる範囲を表します。*カスケード接続：複数のネットワークスイッチを直列に接続してネットワークの規模を拡大する方法

上記を前提として、物理的セグメント化とは、2 台以上の L2 スイッチを用いて、同一の L2 スイッチを共有することなく、異なる 2 つ以上のネットワークセグメントを構成することを意味します。物理的にセグメント化された 2 つのネットワークセグメントが通信する場合、トラフィックを制御できる機器（ルーター、ファイアウォール）を用いなければなりません。

論理的セグメント化とは、1 台の L2 スイッチにおいて仮想的に分離する機能、VLAN を用いて、異なる 2 つのネットワークセグメントを構成することを意味します。

・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分離可能とする

図 4.3 中の vii)について、あるコンピュータシステムにサイバーインシデントが発生した場合、ネットワーク通信を介して、他のセキュリティゾーンに被害が及ぶ可能性があることから、セキュリティゾーンを速やかに分離する必要があります。一方で、上記の場合においても、船舶の安全航行上重要な機能の中断が起きないことを考慮しなければなりません。そのために、ゾーンを分離した際に、ゾーン内のコンピュータシステムの性能が制限されないようにゾーン設計する必要があります。

規則　X 編 5.4.3(1)(d)i)3)

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。

ゾーン及びコンジット図では、本章の適用範囲内にある各コンピュータシステムを識別できる必要があります。

なお、ゾーン及びコンジット図にすべての通信プロトコルを記載することは必須ではありませんが、ゾーンを区別するために通信プロトコルが関係する場合は、通信プロトコルの記載が必要となる場合もございます。

4-3. サイバーセキュリティデザインの説明

規則　X 編 表 X2.4 番号 7

統合者：提出、完工まで保守　　船主：保守

4-3.1 概要

サイバーセキュリティデザインの説明は、ネットワークレベルおよびデバイスレベルで、防御、対応、復旧の 3 つの要件に寄与する技術的な対策をまとめて説明した文書です。

本資料は、船主が船舶サイバーセキュリティ・レジリエンス計画書を作成する際に、各システムとネットワークに備わっているセキュリティ機能を平易に理解し、必要な参考図書に容易にアクセスできることを目的としています。具体的には、デバイスレベルでは、供給者から受領した機能に関する情報を整理し、必要な文章を紐づけします。ネットワークレベルでは、ゾーン分離の方針、ゾーン間の対策内容、エンドポイントの対策内容、および物理的対策等を整理する作業を行います。

4-3.2 解説

規則　X 編 2.2.3-3.(5)

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。

本資料の要件は、X 編 5.4 に規定されております。本要件は、**4-4.3** にて解説します。

4-3.3 機能要素毎の各要件の解説

本資料では、機能要素毎に定められた要件を満たす必要があります。各要件については、以下で詳しく解説しております。

X 編 5.4.3 防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント　P. 33

X 編 5.4.3(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　P. 35

X 編 5.4.3(4) アクセス制御　P. 38

X 編 5.4.3(5) 無線通信　P. 38

X 編 5.4.3(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 P. 40

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用 P. 43

X 編 5.4.5 対応

X 編 5.4.5(1) インシデント対応計画書 P. 44

X 編 5.4.5(2) 機側、独立及び／又は手動の操作 P. 45

X 編 5.4.5(3) ネットワークの隔離 P. 45

X 編 5.4.5(4) ミニマルリスクコンディションへのフォールバック P. 45

X 編 5.4.6 復旧

X 編 5.4.6(1) 復旧計画書 P. 46

X 編 5.4.6(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 P. 47

防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント

規則　X 編 5.4.3(1)(d) i) 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の簡単な説明。
- 同一セキュリティゾーン内でのコンピュータシステム間のネットワーク通信。説明には，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）に関する説明を含めなければならない。
- 異なるセキュリティゾーン間のコンピュータシステムのネットワーク通信。説明には，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）に関する説明を含めなければならない。また，ゾーン境界デバイスに関する説明も含み，ゾーン境界を通過することが許可されるトラフィック（例えば，ファイアウォールルール）を明示しなければならない。

- セキュリティゾーン内のコンピュータシステムと信頼されていないネットワークとの間のすべての通信。説明には，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）に関する説明を含めなければならない。また，ゾーン境界デバイスに関する説明も含み，ゾーン境界を通過することが許可されるトラフィック（例えば，ファイアウォールルール）を明示しなければならない。

- **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の簡単な説明。**

　各セキュリティゾーン内に含まれるコンピュータシステムについて、名称や用途、目的を明示してください。

- **同一セキュリティゾーン内でのコンピュータシステム間のネットワーク通信。説明には，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）に関する説明を含めなければならない。**
  - 通信の目的：通信の利用目的を簡単に明示してください。
  - 通信プロトコル：通信に使用するプロトコルを明示してください。
  - データフロー：通信の発信元、受信先及びその間を通過するノード（ファイアウォール等）及び通信方向を明示してください。

- **異なるセキュリティゾーン間のコンピュータシステムのネットワーク通信。説明には，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）に関する説明を含めなければならない。また，ゾーン境界デバイスに関する説明も含み，ゾーン境界を通過することが許可されるトラフィック（例えば，ファイアウォールルール）を明示しなければならない。**

　ファイアウォールルールを明示する必要があります。ファイアウォールルールとは、ネットワークを通過するトラフィックを制御するために設定される一連のポリシーです。特定のトラフィックを許可または拒否する設定を行うことで、必要な通信のみに制限します。例えば、ファイアウォールルールとして、許可された発信元および受信先の IP アドレス、ポート番号、プロトコルを本資料に記載することが考えられます。

- **セキュリティゾーン内のコンピュータシステムと信頼されていないネットワークとの間のすべての通信。説明には，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）に関する説明を含めなければならない。また，ゾーン境界デバイスに関する説明も含み，ゾーン境界を通過することが許可されるトラフィック（例えば，ファイアウォールルール）を明示しなければならない。**

　デジタル信号（離散信号）及びシリアル通信についても全て含めて記載する必要があります。

X 編 5.4.3(2) ネットワークを防御する防護策

規則　X 編 5.4.3(2)(d) i)

要件なし。

X 編 5.4.3(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

X 編 5.4.3(3)(c)要件の詳細では以下のように述べられています。

規則　X 編 5.4.3(3)(c)

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。

- **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。**

　ウイルス，マルウェア，スパム及び悪意のあるコードから受けるサイバーリスクを低減することを目的として、コンピュータシステムに対策を実装する必要があります。

- **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。**

　Windows や Linux などの汎用 OS を使用する場合は、業界標準のウイルス対策及び／又はマルウェア対策ソフトウェアをインストールし、また、保守及び定期的にアップデートすることが必要です。

　マルウェア対策ソフトウェアにはブラックリスト型とホワイトリスト型の 2 つの方式があります。前者はマルウェアの特徴的なコード(シグネチャ)や不審な振る舞い(ビヘイビア)等を定義ファイルとして保管しており、それと照合することによりマルウェアを検

知しています。この定義ファイルが古くなると新たな脅威に対応できなくなってしまうため、継続的に更新し続ける必要があります。一方で、後者であればあらかじめ許可されるプログラムを指定する必要はありますが、定義ファイルを更新する必要がなく、ソフトウェアの変更に対する対応のみとなります。マルウェア対策ソフトウェアはこれらの特徴を把握したうえで、システムの特性を考慮して選択される必要があります。

- **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。**

　ただし、リアルタイムでタスクを実行することが重要なコンピュータシステムであって、当該ソフトウェアをインストールすることにより要求される機能及びサービスレベルを提供する能力が損なわれる場合は、当該ソフトウェアのインストールは求められません。

- **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。**

　一方で、前項により除外される場合を含めて当該ソフトウェアをインストールできない場合は、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の実装が必要です。

以上が、ウイルス対策およびマルウェア対策に関わる要件となります。上記を踏まえたうえで、サイバーセキュリティデザインの説明には、以下の要件に従って内容を記載する必要があります。

規則　X 編 5.4.3(3)(d) i)

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，悪意のあるコードまた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承認されたメカニズムの概要。
2) マルウェア対策ソフトウェアを含むコンピュータシステムについて，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) 船主の管理システムで実施される運用条件又は必要な物理的保護措置。

- **1) 各コンピュータシステムについて，悪意のあるコードまた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承認されたメカニズムの概要。**

　ここでは、悪意のあるコードまた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セキュリティ機能について、どのようなセキュリティ機能が実装されているか把握できるように、その概要を文書化する必要があると述べています。

　具体的には、対応する脅威や脆弱性について、どのようにセキュリティ機能が動作して

それらを防ぐのかの説明を記載する必要があります。

本項については、X 編 4 章 表 X4.1「18. 悪意のあるコードからの保護」の要件に対して各システムの供給者が講じた対策を参照することができます。詳細は、「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ガイドライン」5 章の「18. 悪意のあるコードからの保護」 (P98)をご覧ください。

- 2) マルウェア対策ソフトウェアを含むコンピュータシステムについて，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。

マルウェア対策ソフトウェアを含むコンピュータシステムである場合には、ソフトウェアのアップデートで対策すべき新たな脅威や脆弱性が発見された際に、ソフトウェアをアップデートする必要があります。また、マルウェア対策ソフトウェアがブラックリスト型の場合には、これに加えてマルウェアの定義ファイルを最新の状態に維持する必要があります。

ここではマルウェア対策ソフトウェアを含むコンピュータシステムについては、当該ソフトウェアを継続的にアップデートする方法を文書化する必要があると述べています。

具体的には、マルウェア対策ソフトウェアのアップデートが必要となる新たな脅威や脆弱性が発見された際に供給者等から提供されるアップデートファイルやパッチファイルについて、入手プロセスや、当該ファイルを適用するプロセスを記載する必要があります。

- 3) 船主の管理システムで実施される運用条件又は必要な物理的保護措置。

ウイルス，マルウェア，スパム及び悪意のあるコードには、船主の管理システムに従って実施される運用や提供される物理的保護措置による対策が必要です。

ここではそれらの運用条件や物理的保護措置によるセキュリティ対策についても文書化する必要があると述べています。

具体的には、以下のような内容です。

運用条件：

侵入検知・防止システム（IDS/IPS）の導入、電子メール，その添付ファイル，ウェブサイトやウェブサービスの利用，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）に対する接続前のマルウェアスキャン、ネットワーク接続の制限などに関する運用面の条件を記載する必要があります。

物理的保護措置：

X 編 5.4.3(3)(c) ii) 要件の詳細に従って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をマルウェアから保護するために実装される，施錠できる部屋や保管庫の中にコンピュータシステムを配置するなどの物理的なアクセス制御の採用や物理ポートのブロックといった物理的防護策について記載する必要があります。

X 編 5.4.3(4) アクセス制御

規則　X 編 5.4.3(4)(d) i)

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。

本項は、アクセス制御により攻撃者からの船舶のシステム及びデータへのアクセスを阻止することを目的としています。アクセス制御には、人員に与えるアクセス権限を制御する論理的な方法と、コンピュータシステムを施錠可能な部屋若しくは管理されたスペースに設置することによる物理的な方法があります。ただし、即時アクセスを必要とするような、船舶の安全な運航に関わるコンピュータシステム（分類 II 又は分類 III）については、権限を与えられた人員が容易にアクセスできるような配慮が必要です。

サイバーセキュリティデザインの説明には、以下の情報を記載してください。

- コンピュータシステムを設置した位置及び物理的アクセス制御の概要
- 即時アクセスを必要とするコンピュータシステムの一覧

X 編 5.4.3(5) 無線通信

無線通信にはローカル通信向けの Wi-Fi や外部通信向けのモバイル通信技術その他の高周波無線通信技術が含まれます。これらは、有線通信と比較して物理的な防御手段を施すことが難しく、信頼されていないデバイスによる傍受や改ざんなどのサイバーリスクを抱えています。このようにサイバーリスクの高い無線通信において，許可されたデバイスのみへの制限，ファイアウォールルール等の明確化により，より強固な要件を要求することを目的とします。

規則　X 編 5.4.3(5)(d) i)

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）。

本要件により、無線ネットワークをどのように実装しているのかをサイバーセキュリティデザインの説明に記載する必要があります。

無線ネットワークの設計条件については、要件の詳細として規定されている、下記の条件

を満たす必要があります。

規則　X 編 5.4.3(5)(c)

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。

- i) 無線ネットワークの暗号化メカニズムの利用

無線ネットワークを利用する場合は、傍受、改ざんのリスクを低減するため、暗号化メカニズムを採用する必要があります。詳細は、「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ガイドライン」5 章の「17. 通信の完全性」 (P96)および「22. 暗号の使用」(P108)をご覧ください。

- ii) 無線通信を行うデバイスが無線通信専用であること（有線通信の禁止）

無線ネットワークに接続するデバイスは、下記の通り独立したセグメントとする必要があります。そのため、他のセグメントとの通信を行う可能性がある有線接続ポートによる接続は禁止する必要があります。そういったポートがある場合はポートブロッカーによる物理的あるいは、ソフトウェアによる論理的な通信防止措置を行って下さい。

- iii) 無線ネットワークの独立したセグメント化

無線ネットワークに接続するデバイスは、有線接続のデバイスに比べて脆弱性が高くなります。そのため、無線ネットワークでインシデントが発生した場合に（Firewall、その他の L3 スイッチ等を用いて）セグメントを分離することで別のセグメントへの被害の拡大を防ぐ必要があります。

- iv) デバイスおよびアクセスポイントの無線アクセスが制御可能であること

無線ネットワークに接続されるデバイスや、それを提供するアクセスポイントは、悪意のあるネットワーク接続を防ぐため、アクセスの認可、監視、使用制限などの制御が可能である必要があります。詳細は、「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ガイドライン」5 章の「9. 無線の使用の管理」 (P76)をご覧ください。

- **v) 無線ネットワーク内の各機器が、デバイスおよびユーザーを識別できること**

無線ネットワークへの攻撃者は、無線通信を増幅する、指向性のアンテナを用いるといった手法で想定外の範囲からのアクセスを行う可能性があります。そのため、有線接続と比較して物理的なアクセス制御が困難であることから認証機能を設ける必要があります。認証の手法については「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ガイドライン」5 章の「5. 無線アクセスの管理」 (P63)をご覧ください

X 編 5.4.3(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

セキュリティリスクの高い，遠隔アクセス制御及び信頼できないネットワークとの通信において，より厳重な対策を施すための要件となります。

規則　X 編 5.4.3(6)(d) i)

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。

- 本章の適用範囲内で, 遠隔アクセス可能な各コンピュータシステム又は信頼できないネットワークとセキュリティゾーンとの境界を介して通信する各コンピュータシステムの識別。
- 各コンピュータシステムについて，該当する場合には 5.4.3(6)c)に準拠した説明。

- **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。**

本項目について、遠隔アクセスを行うデバイスを明示し、各デバイスに対して適切な対策が取られていることを確認するため、以下の要件があります。

- **本章の適用範囲内で，遠隔アクセス可能な各コンピュータシステム又は信頼できないネットワークとセキュリティゾーンとの境界を介して通信する各コンピュータシステムの識別。**

本項目では、サイバーレジリエンスデザインの説明に、各コンピューターシステムが遠隔アクセス可能であるか、また信頼できないネットワークを介した接続が行われるかが記載される必要があると述べられています。

そのため、防御の要件のうち、X 編 5.4.3(1)「セキュリティゾーン及びネットワークセグメント」において記載を要求されている「同一セキュリティゾーン内でのコンピュータシステム間のネットワーク通信。」において、遠隔アクセスが可能なもの、信頼できないネットワークとの通信があるものについては特記する必要があります。

- **各コンピュータシステムについて，該当する場合には 5.4.3(6)c)に準拠した説明。**

遠隔アクセスまたは信頼できないネットワークとの通信が可能なコンピューターシステムについては、そのための対策が必要です。さらに、遠隔からのシステム変更など、遠隔メンテナンスが行われるシステムについては特別な考慮が払われる必要があります。

設計段階で必要な考慮として、遠隔アクセスの可能なデバイスは規則 X 編 5.4.3(6)c)iii)(1)に記載されている対策を実施する必要があります。また、遠隔アクセスによりメンテナンスを行うデバイスは規則 X 編 5.4.3(6)c)iii)(2)に記載されている対策を実施する必要があります。それらの内容を以下に示します。

まず、遠隔アクセスの可能なデバイスは全て、下記を満たすことが要求されます。

- **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に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。**

  船上の権限を持つ乗組員によって接続を管理する必要があるとの観点から、船上の端末から接続を終了することができること、アクセスをするためには船上の責任ある役割による許可が必要なことが定められています。これらは、エンドポイントの機能として権限者によるアクセス許可を求める機能を実装する方法の他に、遠隔アクセスに必要な VPN 装置の電源管理やネットワークケーブル接続の管理といった運用上の方法が採用できます。

  前者については「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ガイドライン」5 章の「35. 信頼できないネットワーク経由のアクセス」 (P139) 、「37. リモートセッションの終了」 (P143)をご覧ください。また、後者については「36. アクセス要求の明示的な承認」 (P141)をご覧ください。

- **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。**

  OT 機器への遠隔アクセスについて、OT 機器側ではセッションが中断される際に「船上のシステム及び機器のサイバーレジリエンスに関するガイドライン」5 章の「41. セッション終了後のセッション ID の無効化」 (P152)といったセッション管理機能を実行することになります。このとき、OT 機器の安全機能やデータが完全性や可用性を損なわずに利用できることが求められます。

- **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。**

  各コンピューターシステムには、監査可能な事象を監査ログとして記録する機能が求められます。これらについて、遠隔アクセスを行うデバイスは遠隔アクセスに関わるイベント（ログイン試行の成功や失敗、アクセス権限の変更、セッションの確立と終了、および接続先など）を記録する必要があります。これらについて、その内容が遠隔アクセスを行う上で十分であり、また記録容量が十分確保されていることが求められます。

  詳細は「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ガイドライン」

5 章の「13. 監査可能な事象」 (P86)、「14. 監査用の記憶容量」(P89)を参照してください。

それらのうち、遠隔でのメンテナンスが行われる可能性があるデバイスは下記を満たす必要があります。

- **陸上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。**

  遠隔アクセスによってメンテナンスを行う際の手順が明らかとなるように、陸上との接続を行うための手順が明記された書類を作成する必要があります。

- **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イベント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。**

  遠隔でのメンテナンスでは、デバイスのソフトウェアをアップデートしたことで、許容できない脆弱性が発生してしまうと現地でのアップデートと比較して大きな悪影響をもたらします。そのため、遠隔の場合には特にアップデートによる影響は事前に確認される必要があります。

- **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）。**

  アップデートの際には、それを受け入れ可能か、受け入れるべきかを船主が判断できるように、供給者による計画を船主が事前に入手できるようになっている必要があります。そのための資料へのサイバーセキュリティデザインの説明には供給者の作成したそれらの文書への参照が含まれる必要があります。

  参照すべき文書の詳細は、「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ガイドライン」6 章の「2. セキュリティアップデートの文書」 (P158)「3. 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」(P160) 「4.セキュリティアップデートの配信」 (P162)をご覧ください。

- **遠隔保守作業中，いかなる時も，権限を有する人員により，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。**

  ソフトウェアの遠隔保守によって不具合が出た場合や中断する必要のある場合には、安全に保守を中断し、元の状態に復旧できるようになっている必要があります。そのため、遠隔あるいは船上の認証された人員による作業の中断、および遠隔保守以前の状態にソフトウェアを復旧する機能が必要です。

- **範囲内にあるコンピュータシステムへの，人間のユーザーによる信頼できないネット**

ワークからのすべてのアクセスには，多要素認証が求められる。

遠隔保守においては、単なる遠隔でのアクセスだけでなく、それによるソフトウェアや設定値などの変更が容易に可能となります。そのため、認証方式としては多要素認証を行うことが求められます。

多要素認証の詳細は、「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ガイドライン」5 章の「31. 使用者(人)の多要素認証」 (P129)をご覧ください。

- **設定可能な回数の遠隔アクセス試行が失敗した後, 次の試行は所定の時間ブロックされるものとする。**

遠隔保守においては、総当たり方式などの攻撃により不正なアクセスが行われることを防ぐために、何回かアクセス試行が失敗した際にはアクセス試行を決まった時間できなくする機能を提供する必要があります。

詳細は、「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ガイドライン」5 章の「33. 失敗したログイン試行」 (P134)をご覧ください。

- **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。**

通信途絶などの理由により接続が中断された場合に、遠隔セッションが終了されずに継続されていると、不正なアクセスにつながってしまう可能性があります。そのため、接続の中断時にはシステムへのアクセスは終了されるような機能が必要となります。

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用

規則　X 編 5.4.3(7)(d) i)

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，規則 X 編表 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。

携帯用及び可搬式デバイスの使用は、鋼船規則 X 編表 X4.1 中 10 に従って、設計上許可された特定の機能又は活動だけに制限されなければなりません。また、可搬式及び携帯用デバイスへの/からのコード及びデータの転送も制限される必要があります。本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おいては、鍵付きのポートブロッカー等の物理的手段によって未使用のポートを許可のないケーブルやデバイスの接続等から保護する必要があります。（コンピュータシステムが当該要件を満足しているかどうかの判断につきましては、メーカーより提出されるセキュリティ機能仕様書（X 編 4.4.1(3)）をご確認ください。）

サイバーセキュリティデザインの説明には、以上のような物理的手段によるインターフェースのポートの保護が必要となるものに関する情報（例えば、インターフェースのポート

の物理的保護が必要となる機器等の一覧など）を含めてください。

なお、鋼船規則 X 編表 X4.1 中 10 に掲げる要求事項の詳細につきましては、IEC 62443-3-3/SR 2.3 をご確認ください。

対応

X 編 5.4.5(1) インシデント対応計画書

規則　X 編 5.4.5(1) d) i)

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（規則 X 編 4.4.1(8) 参照）を含めなければならない。

本項は，船主がインシデント対応の計画を立てるにあたって必要となる情報を，効率的に参照することを目的としています。インシデント対応計画書は船主によって作成されますが，船内のコンピュータシステムは複雑に構成されているため，船主が正確にインシデント対応計画書を作成できるように，船主だけでは知りえない情報を利害関係者から集める必要があります。

また、インシデント対応計画書には、供給者から提供された情報への参照も含める必要があり、各コンピュータシステムと情報が参照できる資料のリストを作成することが要求されます。

規則　X 編 4.4.1(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) ネットワークの隔離（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)）

インシデント対応計画書において参照すべき資料は、規則 X 編 4.4.1(8)に規定する「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」中、(a)、(b)及び(d)です。

表 4.5　インシデント対応に関する情報が参照できる資料のリスト

コンピュータシステム	製品名称	関連する資料

主機制御システム	***	ローカル独立制御（参照番号：***）

X 編 5.4.5(2) 機側，独立及び／又は手動の操作

規則　X 編 5.4.5(2)(d) i)

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。

本項は，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防御される方法の詳細を確認することを目的としています。SOLAS 条約第 II-1 章 31 規則 2.6 には，遠隔制御場所のいかなる部分が故障した場合においても，推進機器をその場で制御できるようにする旨，規定されています。

具体的には，機側制御が遠隔又は自動制御システムから独立していることが分かるような説明や図解をサイバーセキュリティデザインの説明に含める必要があります。

X 編 5.4.5(3) ネットワークの隔離

規則　X 編 5.4.5(3)(d) i)

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。

本項は，各セキュリティゾーンを隔離する方法及び，隔離による影響を明確にすることことを目的としています。これらの情報は，インシデント対応計画書に記すサイバーインシデント発生時の隔離の指示，手順等に利用することができます。

あるセキュリティゾーンにおいてサイバーインシデントが発生した際，そのセキュリティゾーンを人員が迅速に隔離することで，他のセキュリティゾーンへの影響を最小限に抑えることができます。また、他のシステムからのデータに依存して動作するようなシステムでは，セキュリティゾーンを隔離することで，正常に動作しなくなる場合があります。このため，その旨をセキュリティデザインの説明に明示して，埋合せするための方法を示す必要があります。

X 編 5.4.5(4) ミニマルリスクコンディションへのフォールバック

規則　X 編 5.4.5(4)(d) i)

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。

本項は，各コンピューターシステムの安全な状態とはどのような状態であり、どのようにその状態に達するかかを明確にすることを目的としています。ミニマルリスクコンディションへのフォールバックは，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ます。そのため，様々な状況を想定して検討することが求められます。

ミニマルリスクコンディションへのフォールバックとしては，以下が挙げられています。

- **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（5.4.5(4)(c)i)1)）**
  システムを完全に停止させる又は安全な状態へ移行させることによって，サイバーインシデントによる影響を最小限に抑えることが可能となります。
- **システムの切り離し（5.4.5(4)(c)i)2)）**
  システムを切り離すことで，他のシステムへのサイバーインシデントの影響を抑え，被害の拡大を防ぐことが可能となります。
- **制御の他のシステム又は操作者（人）への引き継ぎ（5.4.5(4)(c)i)3)）**
  制御システムに対してセキュリティインシデントが発生した場合，攻撃を受けていないシステムに制御を移す又は人員により直接制御することにより，セキュリティインシデントの影響を最小限に抑えることが可能となります。

復旧

X 編 5.4.6(1) 復旧計画書

規則　X 編 5.4.6(1)(d) i)

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（X 編 4.4.1(8)参照）を含めなければならない。

- 供給者から提供された情報への言及（4.4.1(8)参照）。これは，サイバーインシデントからの復旧計画を確立するために船主が適用することができる。

これは、各コンピュータシステムに対する復旧方法が示された情報への言及を差しております。本情報は、X 編 4 章（UR E27）にて供給者の提出資料として「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」を指しています。

規則　X 編 4.4.1(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) ネットワークの隔離（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)）

復旧計画書において参照すべき資料は、規則 X 編 4.4.1(8)に規定する「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」中、(c)、(e)、(f)及び(g)です。

本要件では、各コンピュータシステムと情報が参照できる資料のリストを作成することが要求されます。

表 4.6　復旧に関する情報が参照できる資料のリスト

コンピュータシステム	製品名称	関連する資料
主機制御システム	***	リカバリープラン（参照番号：***）

X 編 5.4.6(2) バックアップ及び復元の機能

規則　X 編 5.4.6(2)(d) i)

要件なし。

X 編 5.4.6(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

規則　X 編 5.4.6(3)(d) i)

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。

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

これは、各コンピュータシステムに対する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指します。本情報は、X 編 4 章（UR E27）にて供給者の提出資料として「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」を指しています。従って、X 編 5.4.6(1)で要求事項である「各コンピュータシステムと情報が参照できる資料のリスト」を作成することで達成されます。

ClassNK

4-4. 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

規則　X 編 表 X2.4 番号 5

統合者：提出、完工まで保守　　船主：保守

4-4.1 概要

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は、X 編 5 章（UR E26）の適用範囲内のコンピュータシステムをその適用から除外する場合に、当該システムのセキュリティリスクが十分に軽減されるを証明する資料です。

コンピュータシステムについて、本要件にて示された「合格基準」を満たし、かつリスク評価を実施したうえで X 編 5 章（UR E26）を適用する必要がないと本会が判断した場合に、その適用から除外することが認められております。本資料は、適用を除外したコンピュータシステムをリスト化し、以下で解説する「合格基準」及び「追加基準」を満たすことを証明することが求められます。なお、本資料は、供給者ではなく統合者によって作成される必要があります。

4-4.2 解説

規則　X 編 2.2.3-3.(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。

本資料は、X 編 5.5 に要件が規定されております。本要件において、本資料に重要な点を以下に解説します。

規則　X 編 5.5.4-1.

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から除外することは，コンピュータシステムの運用がサイバーリスクに関する業務の安全性に影響を及ぼさないことが保証される場合に限り，本会によって受け入れられる。以下の追加基準を完全には満たしていない場合にも，証拠とともに合理的な説明が提供され，本会が十分であると認めるコンピュータシステムについては，当該除外を受け入れることがある。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。

本資料の作成にあたっては、後述する X 編 5.5.4-1 に示された「合格基準」および 5.5.4-2 に示された「追加基準」を満たすことが求められます。

まず、コンピュータシステムを X 編 5 章（UR E26）の適用対象外とする場合の「合格基準」について解説します。ここでは、合格基準として、計 4 つの要件が規定されています。当該要件は、X 編 4 章（UR E27）および X 編 5 章（UR E26）で求められるサイバーレジリエンスの要件を適用しないコンピュータシステムについて、サイバーリスクの影響および頻度が十分に軽減されていることの基準です。したがって、本要件においては、いかなる軽減および代替手段は認められません。合格基準を満たす場合は、要件を満たした根拠を本資料へ含めて下さい。

次に、コンピュータシステムを X 編 5 章（UR E26）の適用対象外とする場合の「追加基準」について解説します。除外を検討するコンピュータシステムは、上述の合格基準を満たしたうえで、追加基準として規定された計 3 つの要件を原則として満たす必要があります。本追加要件の適合にあたっては、統合者がリスク評価を実施し、リスク評価結果を基に、統合者がその適合の可否を判断することとなります。なお、本会では、リスク評価手法自体の要件は定めておりませんので、当該手法は統合者にて検討し、実施いただくこととなります。リスク評価の結果、追加基準を満たす場合には、要件を満たした根拠を本資料へ含めてください。

また、リスク評価の結果、追加基準を満たしていない場合においても、本会が認める場合に限り、除外が認められることがあります。上記の場合、必要に応じて関連資料を含めたうえで、除外が認められ得ると考える説明を本資料に追記してください。

規則　X 編 5.5.4-2.

システムを本章の適用範囲から除外するためには，以下の基準を満たさなければならない。

(1) コンピュータシステムを隔離しなければならない。（他のシステムやネットワークへの IP ネットワーク接続がない）

(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ポートを持たないものとしなければならない。未使用のインターフェースは論理的に無効にしなければならない。許可されていないデバイスを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，物理的なアクセスが制御されているエリアに配置されていなければならない。

(4) コンピュータシステムは，本章の適用範囲内にある複数の船舶機能を提供する統合制御システムであってはならない。

上記に掲げる「合格基準」は、必ず満たす必要があります。上記の要件を以下に解説します。

(1)　コンピュータシステムを隔離しなければならない。(他のシステムやネットワークへの IP ネットワーク接続がない)

コンピュータシステムは、以下のケースである場合があります。

・他のシステムやネットワークと完全分離（エアギャップ）が設けられている

・他のシステムやネットワークと IP 通信以外で接続されている（シリアル通信等)。

(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ポートを持たないものとしなければならない。未使用のインターフェースは論理的に無効にしなければならない。許可されていないデバイスを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。

LAN ポート、USB ポート及びネットワークポート等のインターフェースポートが存在しない、又は完全に塞ぐ必要があります。また、その他のインターフェースにおいても論理的に無効化し、デバイスとの接続はアクセス制御リスト等により制御する必要があります。

(3)　コンピュータシステムは，物理的なアクセスが制御されているエリアに配置されていなければならない。

物理的なアクセスが制御されているエリアとは、以下のケースが考えられます。

・常時閉とされた区画（例：Fire Station）

・常時船員により監視できる区画（例：船橋、機関制御室）

・鍵等により物理的アクセスが制御される部屋

(4)　コンピュータシステムは，本章の適用範囲内にある複数の船舶機能を提供する統合制御システムであってはならない。

複数の船舶機能を提供する統合制御システムとは、貨物システム及び機関システムの監視・制御が可能な統合型制御監視システム（Integrated Automation System, IAS）等を指します。

規則　X 編 5.5.4-3.

リスクレベルの許容性の評価には，以下の追加の基準を考慮すべきである。

(1)　コンピュータシステムは，分類 III の船舶機能を提供すべきではないこと。

(2)　既知の脆弱性，脅威，コンピュータシステムに影響を与えるサイバーインシデントから派生する潜在的な影響は，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は，その複雑さ，接続性，遠隔アクセスポイントを含む物理的及び論理的なアクセスポイントを考慮して，最小限に抑えられること。

上記（1）から（3）は、統合者が実施したリスク評価の結果を基に、統合者自身が要件への適合の可否を判断したうえで、その根拠を本資料へ含める必要があります。本会は、その根拠を基に、合理的な結果であることを確認します。

4-5. 補完的対策の説明

規則　X 編 表 X2.4 番号 6

統合者：提出、完工まで保守　　船主：保守

4-5.1 概要

X 編 5 章（UR E26）の適用範囲において、X 編 4 章（UR E27）のシステム要件を単独で満たしていないコンピュータシステムに関する情報をまとめた文書です。この資料は、供給者から提供された「セキュリティ機能仕様書」に記載されている**補完的対策**を整理し、それらが本船でどのように実施されているかの詳細を記載するものです。

この資料の目的は、船主が「船舶サイバーセキュリティレジリエンス計画」を策定する際に、各コンピュータシステムに備えるべきセキュリティ機能がどのように達成されているかを（ネットワークレベルや物理的な管理を通じて等）簡潔に理解できるようにするとともに、必要な参考資料に容易にアクセスできることです。したがって、本資料は、「サイバーセキュリティ設計の説明」と関連付けて参照することが推奨されます。

図 4.5 補完的対策の説明

4-5.2 解説

規則　X 編 2.2.3-3.(8)

X 編 5 章（UR E26）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，X 編 4 章（UR E27）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。

各コンピュータシステムの補完的対策は、X 編 4 章（UR E27）の提出資料のひとつであ

る「セキュリティ機能仕様書」にて言及されています。コンピュータシステムに本対策が採用されている場合、「補完的対策の説明」にそれに関する情報を含める必要があります。含まれる情報として、コンピュータシステムの名称、該当するシステム要件及び採用された補完的対策が挙げられます。

以下に、補完的対策の説明における一例を示します。

例　可搬式及び携帯用デバイスの使用の管理

X 編 4 章（UR E27）のシステム要件では、可搬式及び携帯用デバイスの使用制限及び転送制限の機能をコンピュータシステムに実装する旨、規定されています。可搬式及び携帯用デバイスとは、持ち運び可能な装置であり、例えば USB メモリが該当します。

本機能の目的は、可搬式又は携帯用デバイス経由でマルウェアに感染するリスクを低減することです。ただし、何らかの理由により本機能を実装できない場合、本機能に代替する措置として、「可搬式及び携帯用デバイスを使用する前に、専用のハードウェア等によりマルウェアのスキャン及びクリーンアップすること」を使用者に対して義務づけることで、本機能の目的が達成され、当該要件を満たすこととなります。

4-6. 船舶サイバーレジリエンス試験要領書

規則　X 編 表 X2.4 番号 7

統合者：提出、試運転段階で実証　　船主：保守、定期検査で実証

4-6.1 概要

船舶サイバーレジリエンス試験要領書は、ネットワーク及び各コンピュータシステムのセキュリティ機能の動作検証するための試験方案です。本資料で示される試験は、船舶建造中では試運転段階にて統合者によって実施され、就航後では定期検査にて船主により実施される必要があります。

4-6.2 解説

規則　X 編 2.2.3-4.(2)(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。

本資料の詳細は、X 編 5.4 に規定されております。本要件は、**4-6.3** にて解説します。

規則　X 編 2.2.3-4.(2)(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。

本資料にて実施される各コンピュータシステムのセキュリティ機能の確認試験について、X 編 4 章（UR E27）の承認プロセスを通して正常に実施されている場合、当該試験を省略することが可能です。一方で、試験の省略の可否に関わらず、試験方法については本資料に含める必要があります。これは、前述に示した通り船主が実施する定期検査にも使用されるためです。また、各コンピュータシステムのセキュリティ機能について、本機能に代替する

補完的対策が採用されている場合、X 編 4 章（UR E27）の承認プロセスでの実証に関わらず、省略が認められておりません。補完的対策の試験方法を本資料へ含めたうえで、本試験を実証する必要があります。

規則　X 編 2.2.3-4.(2)(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。

上述した通り、各コンピュータシステムのセキュリティ機能について、本機能に代替する補完的対策が採用されている場合、本対策の試験方法を含める必要があります。各コンピュータシステムにおける試験方法については、X 編 4 章（UR E27）の提出資料のひとつである「セキュリティ機能試験要領書」に記載されております。

規則　X 編 2.2.3-4.(2)(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

この資料には、各要件の実証試験に対する試験条件、試験機器、初期条件、試験手法、予想される試験結果等を含む必要があります。さらに、試験中に試験結果や所見を記録するための記入欄を含める必要があります。

4-6.3 機能要素毎の各要件の解説

本資料では、機能要素毎に定められた要件を満たす必要があります。各要件については、以下で詳しく解説しております。

X 編 5.4.2 識別

X 編 5.4.2(1) 船舶資産インベントリ　P. 57

X 編 5.4.3 防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント P. 58

X 編 5.4.3(2) ネットワークを防御する防護策 P. 59

X 編 5.4.3(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 P. 61

X 編 5.4.3(4) アクセス制御 P. 62

X 編 5.4.3(5) 無線通信 P. 62

X 編 5.4.3(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 P. 63

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用 P. 66

X 編 5.4.4 検知

X 編 5.4.4(1) ネットワーク動作の監視 P. 67

X 編 5.4.4(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 P. 71

X 編 5.4.5 対応

X 編 5.4.5(2) 機側、独立及び／又は手動の操作 P. 72

X 編 5.4.5(3) ネットワークの隔離 P. 73

X 編 5.4.5(4) ミニマルリスクコンディションへのフォールバック P. 73

X 編 5.4.6 復旧

X 編 5.4.6(1) 復旧計画書 P. 74

X 編 5.4.6(2) バックアップ及び復元の機能 P. 74

X 編 5.4.6(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 P. 75

識別

X 編 5.4.2(1) 船舶資産インベントリ

規則　X 編 5.4.2(1)(d) iii)

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。）

船舶サイバーレジリエンス試験要領書には、船舶資産インベントリ及び船舶資産インベントリにリストアップされるソフトウェアが適切に管理されていることを本会検査員に実証するための要領を定める必要があります。

船舶サイバーレジリエンス試験要領書に以下の実証のための要領を定め、試運転段階までに本会検査担当支部に実証する必要があります。

1) 船舶資産インベントリに記載すべき内容について、記載が完了していること。
2) 本規則の適用となるすべてのコンピュータシステムが船舶資産インベントリに含まれていること。
3) 船舶資産インベントリに記載されている各ソフトウェアを、船舶サイバーセキュリティ・レジリエンス計画書に計画されるソフトウェアアップデートの管理に基づいてアップデートするための手順。

また、試運転段階において定めた要領に基づいて試験を実施し、本会検査員に実証する必要があります。

なお、本会検査員への実証については、以下のような方法を組み合わせて実施いただけますので、これらの実施に必要な手順を記載してください。

・検査員の直接照合による確認
　船舶資産インベントリの内容と本船上の状況を検査員が直接確認して照合する方法です。
・自動化ツールの活用
　船舶資産インベントリのデータを自動的に確認するツールを活用し、最新の情

報を取得する動作を検査員が確認する方法です。

手順については、各コンピュータシステムのマニュアル等を参照することも可能です。その場合は船舶サイバーレジリエンス試験要領書（又は船舶資産インベントリ）に参照先を明記してください。

防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント

規則　X 編 5.4.3(1)(d) iii)

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，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，設置された設備が承認された設計に従ってセキュリティゾーンに分類されていることを検査員が保証する他の方法によっても実施されることがある。
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，ファイアウォール規則の評価，ポートスキャン等によって行うことができる。

- **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，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，設置された設備が承認された設計に従ってセキュリティゾーンに分類されていることを検査員が保証する他の方法によっても実施されることがある。**

この試験は、承認資料に明示されたネットワークゾーン通りに設置・配線されていることを確認します。確認方法については、以下が例として挙げられます。

- 物理的な設備の検査：

ゾーン及びコンジット図等を参照しながら、現場にて設備及び配線の設置状況を確認します。

- ネットワークスキャン：

ネットワークスキャンを実施して、セキュリティゾーン内で稼働している通信やポートを識別します。具体的には、ネットワークスキャン「サイバーセキュリティ設計の説明」内に記載された各コンピュータシステムの通信プロトコル及びデータフローのとおりとなっていることを、ネットワークスキャンのツールを用いて確認します。ネットワークスキャンについては、Nmap 及び Wireshark といったツールが用

いられることとなります。

- Ping テスト：

　先に述べたネットワークスキャンの代替手段として、Ping テストが挙げられます。本テストは、ネットワーク上で他のデバイスとの接続性を確認するための基本的な診断ツールを用いた確認です。本ツールにより、許可される／拒否される IP アドレス等を確認します。

- 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。

　この試験は、セキュリティゾーン境界を通過するトラフィックが「サイバーセキュリティ設計」に記載されたもののみ通過することを確認するための試験です。具体的には、以下が一例として挙げられます。

- ファイアウォールルールの評価：

　セキュリティゾーン境界デバイスが、設計されたファイアウォールルールに従って設定されていることを確認します。具体的には、本船に設置されたファイアウォールが「サイバーセキュリティ設計の説明」に記載されたファイアウォールルールのとおりに設定されていることを確認することが一例として挙げられます。

- ポートスキャン：

　ポートスキャンは、ネットワークに接続された機器のポートに接続を試み、応答を調べる方法です。ポートスキャンにより、どのポートが開いているか／閉じているかを確認することで、トラフィックが通過するポートを確認できます。ポートスキャンを実施するためのツールとして、Nmap が挙げられます。

X 編 5.4.3(2) ネットワークを防御する防護策

規則　X 編 5.4.3(2)(d) iii)

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フローレートからの保護を保証するサービス拒否（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）を対象としなければならない。
3) 例えば，分析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)（両方ともハードニング指針）を参照すること。

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基づい

て省略してもよい。

- 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）

この試験では、ファイアウォール等のゾーン境界デバイスが DoS 事象を検出してブロックすることを確認します。本試験は、ネットワーク設計上、ゾーン境界デバイスによって DoS 事象をブロックするような設計の場合に要求されます。具体的には、実際に DoS 事象を発生させることで、ゾーン境界デバイスが本事象をブロックすることを確認します。本試験に使用されるツールとして、商用ツール及びオープンソースツールが挙げられます。

- 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フローレートからの保護を保証するサービス拒否（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）を対象としなければならない。

この試験では、DoS 事象による意図的に生成された高負荷のデータフローから、ネットワーク及びコンピュータシステムが耐え得ることを確認します。具体的には、商用ツール及びオープンソースツール等の外部ツール等を用いて、大量のデータパケットを送信することで、ネットワーク及びコンピュータシステムがそれらの処理能力を維持することを確認します。この試験では、ネットワークのフラッディング及びアプリケーション層攻撃を対象とする必要があります。

- ネットワークのフラッディング：

  許容範囲を超える量のデータが送信されることで、ネットワークを動作不能に陥らせる状態のことを指します。ネットワークの帯域幅が急激に消費された場合にネットワークがどの程度正常に機能を維持できるかを確認します。

- アプリケーション層攻撃：

  アプリケーションの脆弱性を悪用したサイバー攻撃です。大量のリクエストを受けた際に、アプリケーションがどの程度応答性を維持できるか、そしてどの速度でリクエストを処理できるかを評価します。

なお、各コンピュータシステムが X 編 4 章（UR E27）の承認を受けている場合、当該試験の省略が可能です。省略する場合は、X 編 4 章（UR E27）により規定された以下のセキュリティ機能に関する試験結果を添付の上、機関部へお問い合わせいただくことになります。

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 事象発生中にも，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。 (IEC 62443-3-3/SR 7.1)

3) 例えば，分析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)（両方ともハードニング指針）を参照すること。

この試験では、各コンピュータシステムにおける「不要な機能，ポート，プロトコル及びサービス」が削除又は禁止されていることを確認します。「不要な機能，ポート，プロトコル及びサービス」は、X 編 4 章（UR E27）表 X4.1 番号 30 にて、必要最小限とされた上で、同章 4.5.8 にて、供給者が推奨するセキュリティ構成を記載したハードニング指針が作成されています。したがって、この試験では、上記に基づいたセキュリティ構成が変更されていないことを確認します。具体的には、以下の方法が一例として挙げられます。

- 分析評価：

  コンピュータシステムの設定画面にて、プロトコル等の使用状況を確認し、禁止されているものが含まれていないことを検証する。

- ポートスキャン：

  先に述べた Ping テストなどを実施することになります。

なお、各コンピュータシステムが X 編 4 章（UR E27）の承認を受けている場合、当該試験の省略が可能です。省略する場合は、X 編 4 章（UR E27）により規定された以下のセキュリティ機能に関する試験結果を添付の上、機関部へお問い合わせいただくことになります。

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)

X 編 5.4.3(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

規則　X 編 5.4.3(3)(d) iii)

統合者は，船舶サイバーレジリエンス試験要領書（**2.2.3-4.(2)**参照）を協会に提出し，次の事項を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中に実施する場合には省略してもよい。

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）。

この試験では、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を確認します。

実証方法としては、信頼できるマルウェア対策テストファイルによる試験が一例として挙げられます。このファイル、マルウェア対策ソフトの検出能力を評価するために使用されるファイルであり、有名な例としては、EICAR（European Institute for Computer Antivirus Research）テストファイルがあります。このようなテストファイルを用いて、マルウェア対策ソフトが正確にマルウェアを検出できることを実証します。

なお、UR E27（X 編 4 章）の要件に従って既に本会の承認を受けたセキュリティ機能については、本項で要求される船舶サイバーレジリエンス試験要領書の提出及び試験の実施を省略して差し支えございません。

X 編 5.4.3(4) アクセス制御

規則　X 編 5.4.3(4)(d) iii)

統合者は，本会に船舶サイバーレジリエンス試験要領書（X 編 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。

- 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。
- ユーザーアカウントが，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（X 編 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）。

この試験では、コンピュータシステムが権限を与えられた人員だけが立ち入ることのできる場所に配置されていること、ユーザーアカウントが最小権限の原則に従って設定されていること、期間限定で有効なアカウントが不要になった際に削除されていることを確認します。

船舶サイバーレジリエンス試験要領書には、以下を記載する必要があります。

・各コンピュータシステムの設置場所及びそこに立ち入ることのできる人員
・各コンピュータシステムに施された最小権限の原則に従った設定の概要
・各コンピュータシステムに設定された一時的なアカウントの一覧及びその有効期限

X 編 5.4.3(5) 無線通信

無線通信にはローカル通信向けの Wi-Fi や外部通信向けのモバイル通信技術その他の高周波無線通信技術が含まれます。これらは、有線通信と比較して物理的な防御手段を施すことが難しく、信頼されていないデバイスによる傍受や改ざんなどのサイバーリスクを抱えています。このようにサイバーリスクの高い無線通信において，許可されたデバイスのみへの制限，ファイアウォールルール等の明確化により，より強固な要件を要求することを目的とします。

規則　X 編 5.4.3(5)(d) iii)

統合者は，船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)参照）を本会に提出し，次の事項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中に実施する場合には省略してもよい。

1) 権限を有する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) セキュリティで保護された無線通信プロトコルは, 各供給者によって承認された文書に従って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）。

- 1) 権限を有するデバイスのみがネットワークにアクセスできること。

この試験は、無線通信に関する要件の詳細 X 編 5.4.3(5)(c)のうち 4 項(無線アクセスの制御)および 5 項(無線ネットワークにおける認証)を確認するために実施します。詳細は本ガイドラインの 4 章 3 節の防御「無線通信」に記載があります。

4-3 サイバーセキュリティデザインの説明
- X 編 5.4.3(5) 無線通信
P. 38

具体的な手法としては、正規の識別子と認証コードによりログインができ、非正規のものではログインできないことを確認します。その他、MAC アドレス等による使用制限の機能がある場合、その機能を確認します。

- 2) セキュリティで保護された無線通信プロトコルは，各供給者によって承認された文書に従って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）。

この試験は、暗号化や認証に関する無線通信プロトコルが供給者の設計に従って正しく機能しているかどうかを確認するために行います。これにより、無線通信に関する要件の詳細 X 編 5.4.3(5)(c)のうち 1 項(無線アクセスの暗号化)および 5 項(無線ネットワークにおける認証)を確認できます。

具体的な手法としては、アクセスポイントに接続された無線通信のプロトコルを表示することによって実施します。規則に記載されているネットワークアナライザーツールとしては、無線通信のプロトコルを表示する機能を持つものを選ぶ必要があり、例として Wireshark などが挙げられます。

X 編 5.4.3(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

セキュリティリスクの高い，遠隔アクセス制御及び信頼できないネットワークとの通信において，それぞれより厳重な対策を施すための要件となります。

規則　X 編 5.4.3(6)(d) iii)

統合者は，船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)参照）を本会に提出し，次の事項を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，通信プロトコルをより安全でないバージョンとすることができないこと。(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ること。
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できること。
6) 遠隔セッションはセキュリティイベントとして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)

統合者は，船舶サイバーレジリエンス試験要領書（2.2.3-4.(2)参照）を本会に提出し，次の事項を実証しなければならない。

本項目について、試運転段階においてその機能を確認するために、下記の内容を含む試験試験要領を作成し、試運転段階における試験を実施する必要があります。

- **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，通信プロトコルをより安全でないバージョンとすることができないこと。(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)**

本項目は、X 編 4 章の信頼できないネットワークとの通信を行う機器への要求を満足していることを確認する方法を記載することを求めています。

具体的な手法として Wireshark などのネットワークプロトコルアナライザーツールを使うことで実施が可能であることが示されています。

- **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。**

遠隔保守においては、単なる遠隔でのアクセスだけでなく、それによるソフトウェアや設定値などの変更が容易に可能となります。そのため、認証方式としては多要素認証を行うことが求められます。

多要素認証の詳細および確認の手段は、「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ガイドライン」5 章の「31. 使用者(人)の多要素認証」 (P129)をご覧ください。

- **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。**

遠隔保守においては、総当たり方式などの攻撃により不正なアクセスが行われること

を防ぐために、何回かアクセス試行が失敗した際にはアクセス試行を決まった時間できなくする機能を提供する必要があります。また、アクセス試行の前には、システムの遠隔ユーザーに対して同意を求めるメッセージを表示する必要があります。

アクセス試行のブロックに関する詳細は、「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ガイドライン」5 章の「33. 失敗したログイン試行」 (P135)を、メッセージに関しては「34. システム使用通知」(P136)をご覧ください。

この機能を確認するため、本試験では不正な認証情報を利用したアクセス試行を規定の回数繰り返しアクセス試行が制限されること、アクセス試行の前に同意を求める通知が表示されることを検証します。

- 遠隔接続は，船上の責任者によって明示的に許可されること。

不用意な、あるいは悪意のある遠隔接続により意図しないシステムの混入が起こることを防止するため、遠隔接続をされる際には、明示的な許可が必要となります。

詳細は、「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ガイドライン」5 章の「36. アクセス要求の明示的な承認」 (P141)をご覧ください。

- 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できること。

遠隔接続では、通信の状態を管理するために接続確立から切断までの一連の動作における処理状況を保管するためにセッションとしてそれぞれの処理状況を保管します。このセッションが必要でなくなったあともセッションを保管しておくとなりすましの原因となるため、その場合にはこれを終了し無効化することで終了したセッションからのアクセスを拒否する必要があります。

試験においては各機器が設定された一定時間経過後にセッションが自動的に終了する（タイムアウトする）か、手動でセッションの終了が可能であるかを確認します。

詳細は、「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ガイドライン」5 章の「37. リモートセッションの終了」 (P143)、「40. セッションの完全性」(P150)、「セッション終了後のセッション ID の無効化」(P152)をご覧ください。

- 遠隔セッションはセキュリティイベントとしてログに記録されること。（表 X4.1 中 13）

遠隔接続が可能なシステムにおいては、サイバーインシデントの発生時における遠隔接続からの侵入経路を確認するために、接続先や接続/切断時刻の記録が残される必要があります。そのため、信頼できないネットワークとの通信があるデバイスにおいてはそれらを記録する機能があるかどうかを試験時に確認する必要があります。

詳細は、「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ガイドライン」5 章の「13. 監査可能な事象」 (P86)、「35. 信頼できないネットワーク経由のアクセス」(P139)をご覧ください。

- 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）

遠隔接続は、供給者によって保障された方法に基づき実施される必要があります。そのため、X 編 4.4.1(3)により供給者が作成しているセキュリティ機能仕様書に遠隔接続のための方法が記載されていることを確認する必要があります。

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用

規則　X 編 5.4.3(7)(d) iii)

統合者は，船舶サイバーレジリエンス試験要領書（鋼船規則 X 編 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, 権限を与えられたもの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。

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ます。

この試験では、上記の事態を避けるために、携帯用及び可搬式デバイスの使用を制限する機能が正しく実装されていることを確認します。具体的には、下記に示すような試験を行っていただく必要がございます。

- **1) 携帯用及び可搬式デバイスを使用するのは、権限を与えられたものに限られていること。**

　携帯用及び可搬式デバイスの使用を、限られた人員に制限していることを示した文書等を確認します。

- **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。**

　インターフェースのポートを使用できるデバイスが特定の種類のものに制限されていることを示した文書等を確認し、そのデバイスを確認します。可能であれば、テストによって制限されていることを確認します。

- **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。**

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を示した文書等を確認します。可能であれば、本要件を満足していることをテストによって確認します。

- **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。）**

WindowsOS であれば、コントロールパネルの設定で、自動実行が無効化されていることを確認します。独自 OS の場合は、自動実行が行われないことを仕様書等によって確認し、可能であれば、実行されないことをメーカーのテスト方法に従って確認します。

- **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。**

携帯用及び可搬式デバイスがネットワークを利用する場合、その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を仕様書等で確認します。可能であればメーカーのテスト方法に従った確認や設定画面等の確認を行います。

- **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。**

コンピュータシステムの使用されないインターフェースのポートは、コンピュータシステムの設定等を含む論理的な手段またはポートブロッカー等の物理的手段によりブロックされ、使用できない状態になっている必要があります。本試験では、前者を採用していた場合にその使用を制限している設定等を確認します。

- **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。**

コンピュータシステムの使用されないインターフェースのポートは、コンピュータシステムの設定等を含む論理的な手段またはポートブロッカー等の物理的手段によりブロックされ、使用できない状態になっている必要があります。本試験では、後者を採用していた場合にポートブロッカー等の物理的手段によりブロックされ、使用できない状態になっていることを目視などで確認します。

検知

X 編 5.4.4(1) ネットワーク動作の監視

規則　X 編 5.4.4(1)(d) iii) 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。

本項目の目的は、サイバー攻撃の影響を検知することで早期に対応、復旧を行い、サイバーレジリエンスを向上させることにあります。また、サイバー攻撃には、実際の被害に至らないもの（例えば、侵入・通信の試行など）も含まれます。このような兆候の検証を行うことで、コンピュータシステムの防御機能をより高めることもその目的の一つです。

本項目における試験のうち、X 編 4 章に基づき本項目の要求に相当する試験を確認済みであるものについては省略が可能です。

- 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。

本項目は、要件の詳細におけるネットワーク接続の監視機能が正しく機能していることを実証し、セキュリティポリシーを遵守するために行います。

ネットワーク接続を監視し接続情報を記録/分析することで、不審なアクティビティや不正なアクセスといったセキュリティポリシーへの違反を発見できます。これにより脅威にいち早く対処し、被害を最小化することができます。記録すべき内容としては

・各コンピュータシステムへの認証の成功/失敗状況
・各コンピュータシステムへのアクセス状況/アクセス先(IP, ポート)/エラー状況
・各コンピュータシステムからの設計から逸脱したネットワークへのアクセス

等が挙げられます。

本試験は、システム内あるいはシステム間のネットワーク接続を切断することにより実施します。この際にネットワーク接続が切断されたことを示す警報が発され、そのことを示す記録が監査記録として残されることを確認します。

- 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。

要件の詳細における過度のトラフィックの監視及び検知ができることを実証するために行います。本要件により、DoS 攻撃/DDoS 攻撃への対応ができます。

DDoS 攻撃を受け、多量のデータを受信するとトラフィックが一時的に多くなります。このトラフィックを監視し、その異常な増加を検知することで DDoS 攻撃を受けていることを検知できます。また、ソフトウェア自身がシステム攻撃に加担させるようなマルウェアに感染した場合、内部の他システムに対して DoS 攻撃を仕掛けてしまうことが想定されます。トラフィックを監視することで、このような攻撃を仕掛けていないかについても監視することができます。

本試験では、過度なトラフィックの模擬として多量のパケットを送付する試験を行い、それによるトラフィックの増加が検知・警報され、警報の監査記録が行われることを確認します。

- 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）。

本項は過度なトラフィックが加えられた場合でも、保護対象のシステムへの影響が最小化されていることを実証するために行います。

本試験では、ネットワークストームにシステムが晒された際の挙動を確認することで、そのような状況下でもセキュリティ機能の保護あるいはシステムそのものの設計により、システム全体が正常に作動する、あるいは危険な動作を引き起こさないことを実証します。本試験は、防御における要件「5.4.3(2) ネットワークを防御する防護策」における試験と同時に実施ができます。詳細は本ガイドライン 4 章の 7 節、防御の第 2 項「5.4.3(2) ネットワークを防御する防護策」をご覧ください。

6-7 船舶サイバーレジリエンス試験要領書
- X 編 5.4.3(2) ネットワークを防御する防護策
P. 59

なお、本試験は X 編 4 章表 X4.1 中#24 の「サービス保護攻撃からの保護」に関する試験が実施済みであることが証明されたシステムにおいては省略可能です。

- 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）

本項目はネットワーク接続やデバイス管理活動がセキュリティ機能により正しく記録されることを実証するために行います。これにより、侵入が行われた際の経路や被害状況を正しく判断して、復旧後の対応を迅速に行うことを目的としています。また、防御の面においてもこれらの検知情報を利用することで意図していない管理情報の変更を発見/遮断することも可能となります。

記録すべき内容としては

・各コンピュータシステムのシャットダウン試行/動作状況（死活監視など）
・各コンピュータシステムのリソース状況（プロセッサ/メモリ使用率など）
・各コンピュータシステムの管理者権限/環境設定/アカウント設定の変更
・クリア可能なログのクリア記録
・各コンピュータの物理的な侵入記録（ストレージ等へのアクセス、電源操作など）

等が挙げられます。

本試験では、システム設計者の仕様において記録が行われるネットワーク接続およびデバイス管理活動における監査記録の項目について、監査記録を行うべき操作により実際に記録が生成されることを確認します。なお、本試験は X 編 4 章表 X4.1 中#13 の「監査可能なイベント」に関する試験が実施済みであることが証明されたシステムにおいては省略可能です。

- **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。**

侵入検知システム(Intrusion Detecting System: IDS)とは、ネットワーク通信においてファイアウォールを通過した通信のうち、悪意があるもの、あるいは内部に侵入したプログラムによりネットワーク内部で悪意のある通信を行っていると推定されるものを検知・警報するシステムを指します。ファイアウォールとの違いは、ファイアウォールがネットワークの境界に置かれ、境界をまたがる通信を監視しているのに対して、IDS は境界の内側での通信も監視している点です。

このような IDS を設置する場合、下記の要件を満足する必要があります。

規則　X 編 5.4.4(1)(c) 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。

- **当該 IDS は，それぞれのコンピュータシステムの供給者により認められていなければならない。**

本項は、セキュリティ機能とネットワークとの互換性を保つことを目的としています。

IDS はセキュリティ機能を発揮するためにネットワークを監視するシステムです。しかし、船舶のシステムアーキテクチャに適合するように IDS が設計されていなければ、IDS が正常に動作しない危険性や最悪の場合コンピュータシステムに対して不正な動作を行わせてしまう危険性があります。

- **当該 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起動しないものでなければならない。**

本項は、システムの可用性を確保することを目的としています。

セキュリティ機能を実行することにより処理装置やネットワークに対する負荷が加わると、OT 機器の動作に影響を与える可能性があります。また、IDS が能動的にネットワーク遮断等を行う IDS/IPS として設計されていた場合、ネットワーク遮断により重要な機器の通信に不具合が生じ、船舶の運航上のリスクにつながる可能性があり、誤検知の場合

にはリスクが増大する結果をもたらしてしまいます。そのため、船舶の OT 機器として侵入検知システムを実装する場合は受動的な動作が望ましいと考えられます。

- **関係する人員は，当該 IDS の使用に関して，訓練を受けて資格を有するべきである。**

本項は、IDS を効果的に運用することを目的としています。

IDS による攻撃兆候の検知について、その効果を最大限発揮させるためには IDS の種々の機能を適切に利用できる必要があります。例えば、サイバー攻撃の兆候を発見するためには IDS により検知された接続情報を分析する必要がありますが、それにはネットワークに関する専門知識が必要です。また、妥当な検出基準の設定により、IDS の誤検知を防止するためにもネットワークに関する専門知識が役に立つと考えられます。

以上の内容を踏まえて、本試験では侵入検知システムの仕様により検出が行われる動作を実行することにより、IDS の侵入検知時の応答を確認します。この際、侵入遮断が行われるなどによりコンピュータシステムの動作に影響が与えられないことが求められます。

規則　X 編 5.4.4(1)(d) iii)(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。

本項は、要件の詳細の前半で掲げるネットワークの監視手段に加えて IDS を実装する場合に適用されます。本会の承認プロセスにおいては、ネットワークの監視手段は図面審査と検査立会の両方を受けることになりますが、IDS を実装する場合はそれらに加えて IDS に対する図面審査と検査立会が必要となります。

IDS に関してはセキュリティ機能とコンピュータシステムまたはネットワークとの互換性を保つために、それぞれのコンピュータシステムの供給者により認められていること、IDS を用いて攻撃の兆候を検知するためには専門知識が必要であることから、関係する人員は訓練を受けて資格を有するべきであることが規定されています。

X 編 5.4.4(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

規則　X 編 5.4.4(2)(d) iii)

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。

規則　X 編 5.4.4(2)(c)

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，すべての要求される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。

本要件はセキュリティ機能の正常性の確認、不具合の発見、セキュリティ機能の改善を目的としています。

運用者が定期的にセキュリティ機能の正常動作ができているかを確認することでセキュリティ機能の保全を確実なものにすることができます。また、セキュリティ機能に異常が見つかった際にはサイバー攻撃に脆弱となっている可能性があるので、これを早期発見し対処することが必要です。さらに、セキュリティ機能の動作検証を定期的に実施することで機能の向上につなげることもできます。

試験要領書には、コンピューターシステムのセキュリティ機能の検証手順を記載する必要があります。この手順を記載するためには、各コンピューターシステムが X 編 4 章 表 X4.1 の No.19 に基づき仕様書に記載しているセキュリティ機能の検証方法を参照することが有効です。

対応

X 編 5.4.5(1) インシデント対応計画書

規則　X 編 5.4.5(1)(d) iii)

要件なし。

X 編 5.4.5(2) 機側，独立及び／又は手動の操作

規則　X 編 5.4.5(2)(d) iii)

統合者は，本会に船舶サイバーレジリエンス試験要領書（規則 X 編 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，鋼船規則 X 編 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。

本項は，船舶の安全な運航のために必要な機側制御が，遠隔又は自動制御システムから独立して操作できることを文書により確認することを目的としています。

船舶サイバーレジリエンス試験要領書には、対象のコンピュータシステムを機側制御に切り替える手順を示し、当該コンピュータシステム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合格基準とする必要があります。

X 編 5.4.5(3) ネットワークの隔離

規則　X 編 5.4.5(3)(d) iii)

統合者は，本会に船舶サイバーレジリエンス試験要領書（規則 X 編 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，規則 X 編 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。

本項は，ネットワークを隔離しても，各コンピュータシステムが適切な運用上の機能性を維持することを文書により確認することを目的としています。

船舶サイバーレジリエンス試験要領書には、ネットワークの論理的及び／又は物理的な隔離の手順を示し、各コンピュータシステムが通信なしで適切に動作することを合格基準とする必要があります。

X 編 5.4.5(4) ミニマルリスクコンディションへのフォールバック

規則　X 編 5.4.5(4)(d) iii)

統合者は，本会に船舶サイバーレジリエンス試験要領書（規則 X 編 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，（規則 X 編 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，規則 X 編 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，規則 X 編 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。

本項は，ミニマルコンディションへフォールバックする機能により，サイバーインシデントに対応できることを文書により確認することを目的としています。

当該試験は，規則 X 編 5.4.4(1)(d)iii）に規定する，ネットワーク動作の監視に関する試験と同時に実行することが出来ます。また，当該試験にはサービス拒否（DoS）攻撃を含む必要があります。船舶サイバーレジリエンス試験要領書には、DoS 攻撃を実施する手順を示し、攻撃を受けた際にどのようなフォールバックを行うかを示してください。各コンピュータシステムが、DoS 攻撃を受けた後に重要なサービスへの出力を維持しつつ、適切に動作す

ることを合格基準としてください。

復旧

X 編 5.4.6(1) 復旧計画書

規則　X 編 5.4.6(1)(d) iii)

統合者は，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)に規定され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中に実施する場合には省略してもよい。

- **5.4.6(2)及び(3)に規定され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本会に実証しなければならない。**

　ここでの要件は、X 編 5.4.6(2)及び(3)に示されております。詳細については、以下をご参照ください。

X 編 5.4.6(2) バックアップ及び復元の機能

規則　X 編 5.4.6(2)(d) iii)

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中に実施する場合には省略してもよい。

- **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**

　本試験では、各コンピュータシステムのバックアップ及び復元の手順及び指示を実証することが規定されています。具体的には、X 編 4 章（UR E27）の提出資料である「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」に従ってバックアップ及び復旧の試験を実施いただくことになります。

　なお、各コンピュータシステムが X 編 4 章（UR E27）の承認を受けている場合、当該試験の省略が可能です。省略する場合は、X 編 4 章（UR E27）により規定された以下のセキュリティ機能に関する試験結果を添付の上、機関部へお問い合わせいただくことになります。

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 場所特定並びに使用者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)

X 編 5.4.6(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

規則　X 編 5.4.6(3)(d) iii)

シャットダウン，リセット及び復元のための説明書又は手順が確立されていることを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中に実施する場合には省略してもよい。

・シャットダウン，リセット及び復元のための説明書又は手順が確立されていることを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中に実施する場合には省略してもよい。

本試験では、各コンピュータシステムの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の説明又は手順を実証することが規定されています。原則として、各コンピュータシステムに対する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の試験を実施いただくことになります。

なお、各コンピュータシステムが X 編 4 章（UR E27）の承認を受けている場合、当該試験の省略が可能です。上記について、以下のセキュリティ機能に関する試験時に、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の試験が実施されていることが必要となります。省略する場合は、X 編 4 章（UR E27）により規定された以下のセキュリティ機能に関する試験結果を添付の上、機関部へお問い合わせいただくことになります。

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)

4-7. 船舶サイバーセキュリティ・レジリエンス計画書

規則　X 編 表 X2.4 番号 8

統合者：―　　船主：提出後保守、定期的検査で実証

4-7.1 概要

船舶サイバーセキュリティ・レジリエンス計画書は、X 編 5 章（UR E26）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資料です。船主は、本資料にプロセスをまとめ、船舶の運用期間中においてサイバーセキュリティ及びサイバーレジリエンスを技術的及び組織的に管理することが求められます。

船主は、造船所から引き渡された資料に基づいて、船舶サイバーセキュリティ・レジリエンス計画書を策定する必要があります。具体的には、**4-7.3** に示す通りですが、例えば、以下の内容が含まれます

・セキュリティゾーン内のコンピュータシステムを安全に使用するための手順、
・ゾーン分離やゾーンの保護のために搭載されているネットワーク機器の管理手順、
・アンチマルウェアソフトのアップデート手順、
・セキュリティ機器のアラートへの対応手順、
・　インシデント発生時の対応手順

すなわち、就航後に維持・更新し続けるために、統合者から受領したすべての資料を運用上の手順として落とし込む必要があります。

さらに、作成した運用手順を確実に実施するために、船員および陸上職員を含む人員の訓練など、組織全体での対応が必要です。これには、組織内でのマネジメントシステムが有効であり、例えば、既存の SMS に関連付けることで、効率よく運用することができます。

4-7.2 解説

規則　X 編 2.2.3-5.(7)(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。

本資料の詳細は、X 編 5.4 に規定されております。本要件は、**4-7.3** にて解説します。

規則　X 編 2.2.3-5.(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。

船上のコンピュータシステム、これらのシステムと接続される陸上のコンピュータシステム及びネットワークについて習熟し、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、以下の要件を満たす必要があります。

- **操作手順の作成および実施：**
  システムの一貫した操作を保証するために、具体的な操作手順を作成し、その手順に従って運用することが求められます。
- **定期的な訓練の提供：**
  船内の職員や陸上の関係者が常に最新の知識とスキルを維持するために、システムやネットワークに関する知識や操作方法について、定期的に訓練を実施することが要求されます。
- **船舶内の職員および陸上の関係職員への訓練実施：**
  システムの管理および運用に関わるすべての関係者が必要な知識とスキルを持つために、船内の職員だけでなく、陸上でシステムに関わる他の職員に対しても訓練を実施することが求められます。

規則　X 編 2.2.3-5.(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。

X 編 5 章（UR E26）の適用範囲内であるコンピュータシステム及びネットワーク機器は、定期的な保守を行う等により、正常な動作を維持する必要があります。具体的には、ソフトウェアのアップデートやハードウェアのメンテナンス等が該当します。

4-7.3 機能要素毎の各要件の解説

本資料では、機能要素毎に定められた要件を満たす必要があります。各要件については、以下で詳しく解説しております。本解説では、「計画書に含めるべき内容」と「継続的に作成されるべき記録又は文書化された証拠」について解説するものとなっております。

- **計画書に含めるべき内容：**
  X 編 5.4 中の「運用段階」において要求される、当該計画書が含めるべき管理プロセス。
- **継続的に作成されるべき記録又は文書化された証拠：**
  定期的検査で提出するべき記録。計画書で示された管理プロセスによって作成が義務づけられる記録や手順書で必要となるツールのリストなどが該当する。

X 編 5.4.2 識別

X 編 5.4.2(1) 船舶資産インベントリ　P. 79

X 編 5.4.3 防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント　P. 82
X 編 5.4.3(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　P. 84
X 編 5.4.3(4) アクセス制御　P. 86
X 編 5.4.3(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　P. 89
X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用　P. 92

X 編 5.4.4 検知

X 編 5.4.4(1) ネットワーク動作の監視　P. 95
X 編 5.4.4(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　P. 96

X 編 5.4.5 対応

X 編 5.4.5(1) インシデント対応計画書　P. 97

X 編 5.4.6 復旧

X 編 5.4.6(1) 復旧計画書　P. 100

識別

X 編 5.4.2(1) 船舶資産インベントリ

■ 計画書に含めるべき内容

規則　X 編 5.4.2(1)(d) iv) 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)）

ここでは、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手順を記載する必要があります。

具体的には、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手順について、鋼船規則 X 編 3.6 の変更管理に関する要件に従って実施する必要があります。船舶サイバーセキュリティ・レジリエンス計画書にそのためのプロセスを記載する必要があります。具体的には、以下の内容について含める必要があります。

(1) 対象となるシステム及びソフトウェアコンポーネントのバージョン及びその確認方法

(2) ソフトウェアコンポーネントのマスターファイルと管理方法

(3) 変更による影響度分析

以下を含むこと。

a. 変更の重要度及び影響範囲
b. 既存の資料への影響
c. 必要な検証及び試験
d. 他のステークホルダーへの変更通知の要否
e. 変更前における他のステークホルダーからの承認の要否

(4) ソフトウェアの変更内容

(5) 変更記録

以下を含むこと。

a. 変更の目的
b. 変更点・修正点の内容
c. 影響度の分析
d. 新規のシステムまたはソフトウェアバージョンの設定
e. 試験結果（リリース前、船上試験）

(6) システム変更の検証及び妥当性の確認手順

船舶搭載後に変更を行う場合、検証には以下を含むこと。

a. 変更内容が正しく機能していること

b. 変更内容が他機能又は能力に悪影響を及ぼさないこと

また、コンピュータシステムの改造によってコンピュータシステムの文書に変更がある場合は、当該文書をアップデートする必要があります。

規則　X 編 5.4.2(1)(d) iv) 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)）

以下の要件に対応したソフトウェアアップデートの管理について記述しなければならない。

ここでは、コンピュータシステムのソフトウェアアップデートの管理方法を記載する必要があります。管理については、以下を含める必要があります。

- **脆弱性及びサイバーリスク（5.4.2(1)(b)及び(c)）**

脆弱性及びサイバーリスクとは、コンピュータシステムに存在するセキュリティ上の弱点と、それにより生じるリスクを指します。

船舶サイバーセキュリティ・レジリエンス計画書においては、ソフトウェアのアップデートにより新たに発見された脆弱性を記録し、船舶資産インベントリをアップデートする旨を記載する必要があります。

- **セキュリティパッチ（5.4.3(6)(c)iii)2)）**

セキュリティパッチまたはソフトウェアアップデートとは、ソフトウェアの脆弱性に対応するためのセキュリティ対策機能に対する変更を指し、一般的には比較的小規模の変更をセキュリティパッチ、比較的大規模な変更をソフトウェアアップデートと呼びます。

ソフトウェアの脆弱性は攻撃者の手法の変化、攻撃者の解析による脆弱性の新たな発見等により変化します。このような脆弱性の変化に対応しなければ攻撃者による攻撃が容易になってしまうことから、それに対応してセキュリティ機能は変更される必要があります。

このようなセキュリティパッチまたはソフトウェアアップデートを実施する際には、それらが効果的であること、またこれらを実施したことによって副次的な影響やサイバーインシデントを引き起こさないことを実証するための試験と評価を実施する必要があります。このような試験と評価については供給者によって確認報告書が作成されるので、アップデートに先立ってそれを入手し確認することが求められます。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.2(1)(d) iv) 4)

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。

- 承認された変更管理のプロセスが遵守されていること。

ここでは、鋼船規則 X 編 3.6 の要件で規定された変更プロセスに従って管理されることが求められます。作成される記録としては、変更管理記録が挙げられます。

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

ここでは、既知の脆弱性と機能的な依存性考慮することが求められます。

既知の脆弱性：すでに発見されているセキュリティホールや不具合を指します。当該情報は、一般的にセキュリティアップデート情報に伴って提供される場合があります。

機能的な依存性：あるソフトウェアの機能が他のソフトウェアや他のコンピュータシステムの機能に依存している性質を指します。各コンピュータシステムの機能的な依存性は、一般的に供給者から提供されるユーザーマニュアルに含まれる場合があります。作成される記録又は文書化された証拠としては、アップデート情報や機能的な依存性が記載されたユーザーマニュアル等、及び船舶資産インベントリが挙げられます。

- 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。

船舶資産インベントリは、船上のシステムの一覧として機能します。また、ソフトウェアアップデート等の変更を加える際には脆弱性や機能依存性を参照するための資料にもなります。そのため、資産インベントリは最新に維持されており、それを見ることで現在の船上のシステムが分かるように常にアップデートされる必要があります。

船舶サイバーセキュリティ・レジリエンス計画書には、船舶資産インベントリに変更が必要なハードウェアもしくはソフトウェアの変更があった際に正しくアップデートする必要があることを記載してください。

防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント

■ 計画書に含めるべき内容

規則　X 編 5.4.3(1)(d) iv) 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)）

以下の要件に対応したセキュリティゾーン境界デバイス（例えば，ファイアウォール）の管理について記述しなければならない。

ここでは、ファイアウォール等のセキュリティゾーン境界デバイスの管理方法を記載する必要があります。管理については、以下を含める必要があります。

- **最小権限の原則（5.4.3(2)(a)iii)）**

  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、不可欠な機能のみを備えるように構成する必要があります。

- **明示的に許可されたトラフィック（5.4.3(1)(a)）**

  ゾーンの境界を超えることができるトラフィックは、明示的に許可されたものに限定されることが求められます。トラフィックは、「サイバーセキュリティデザインの説明」内のファイアウォールルールに従って、許可される必要があります。

- **サービス拒否（DoS）イベントに対する防御（5.4.3(2)(a)ii)）**

  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、防御されるものである必要があります。ここでの管理では、このようなイベントに対する把握や定期的な試験について記録書を作成する必要があります。

- **セキュリティ監査記録の検査（5.4.4(1)(c)i)）**

  セキュリティゾーン境界デバイスに保存されたセキュリティ監査記録の確認となります。定期的にセキュリティ監査記録を確認し、異常な事象の発生の有無を把握することが求められます。具体的には、以下の項目を定期的に確認、記録書を作成する必要があります。

1) 過度のトラフィックの監視及び検知
2) ネットワーク接続の監視
3) デバイス管理活動の監視
4) 権限を与えられていないデバイスの接続の有無
5) ネットワーク帯域幅の使用率が，供給者によって異常として指定された閾値を超えた場合の警報の作動の有無（こちらについては、X 編 3.7.2-1.をご参照ください）

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.3(1)(d) iv) 2)

- ゾーン及びコンジット図がアップデートされていること。
- 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。

- ゾーン及びコンジット図がアップデートされていること。

ゾーン及びコンジット図がアップデートされている場合は、当該図面は改造図面として本会機関部へ提出し、承認を得たうえで、保管されている必要があります。

- 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。

ファイアウォール等のセキュリティ境界デバイスが、適切に管理することを示す記録書の作成が求められます。具体的には、以下に掲げる記録書を作成いただく必要があります。

最小権限の原則（5.4.3(2)(a)iii)）

- 機能・ポート・プロトコル・サービス一覧：
  無効化または禁止された機能、ポート、プロトコル、サービスの一覧。
- 変更管理記録：
  無効化または禁止された機能等が作為的又は偶発的に有効化されていないことを確認するための定期的なチェックの記録。

明示的に許可されたトラフィック（5.4.3(1)(a)）

- ファイアウォールルールリスト：
  明示的に許可されたトラフィックのルールが記載されたファイアウォール設定リスト。
- トラフィック許可リスト：
  ゾーンの境界を超えることができるトラフィックの許可リスト。
- トラフィック監視ログ：
  実際のトラフィックが許可されたものに限定されていることを確認するためのログ。

サービス拒否（DoS）イベントに対する防御（5.4.3(2)(a)ii)）

- DoS 防御設定リスト：

ネットワークの DoS 防御設定の一覧。

- DoS イベント監視ログ：

過度なデータフローレートやその他のイベントを監視したログ。

- 試験記録：

DoS イベントに対する防御機能の定期的な試験結果を記録した文書。

セキュリティ監査記録の検査（5.4.4(1)(c)i)）

- セキュリティ監査ログ：

セキュリティゾーン境界デバイスに保存された監査ログ。

- トラフィック監視記録：

過度のトラフィックの監視および検知の記録。

- ネットワーク接続監視ログ：

ネットワーク接続の監視記録。

- デバイス管理活動監視ログ：

デバイス管理活動の監視記録。

- 不正デバイス接続監視記録：

権限を与えられていないデバイスの接続有無の監視記録。

- ネットワーク帯域幅使用率監視記録：

ネットワーク帯域幅の使用率の監視と、異常として指定された閾値を超えた場合の警報作動の有無の記録。

X 編 5.4.3(2) ネットワークを防御する防護策

規則　X 編 5.4.3(2)(d) iv)

特筆した記載事項なし。

X 編 5.4.3(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

■ 計画書に含めるべき内容

規則　X 編 5.4.3(3)(d) iv) 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おいて，本章における少なくとも以下の要件に対応したセキュリティゾーン境界デバイスの管理について記述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，物理的保護（**5.4.3(3)(c)**）
– 携帯用，可搬式，取外し可能メディアの使用（**5.4.3(4)(c)iv**）及び **5.4.3(7)(c)**）
– アクセス制御（**5.4.3(4)**）

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への対策を管理する必要があります。マルウェア対策ソフトウェアをインストールしている場合は適切な管理方法や更新方法に関する説明をし，インストールしていない場合は代替的な物理的保護に関する記述をする必要があります。

船舶サイバーセキュリティ・レジリエンス計画書には、X 編 5.4.3(3)(c)要件の詳細で求められるウイルス，マルウェア，スパム及び悪意のあるコードへの対策に用いられるセキュリティゾーン境界デバイスの管理に関する以下の内容ついて含める必要があります。

- 保守／アップデート
- 運用手順，物理的保護
- 携帯用，可搬式，取外し可能メディアの使用
- アクセス制御

X 編 5.4.3(3)(c)要件の詳細については、4. サイバーセキュリティデザインの説明の 5.4.3(3)を参照ください。

4-3. サイバーセキュリティデザインの説明

X 編 5.4.3(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　P. 35

セキュリティゾーン境界デバイスとは、異なるセキュリティゾーン間を接続し、トラフィックを制御することで不正なアクセスやデータ漏洩などを防ぐハードウェアまたはソフトウェアで、例えば以下のようなものです。

- ファイアウォール
- 侵入検知・防御システム (IDS/IPS)
- VPN 装置
- Web フィルタリング装置
- アプリケーション制御装置

なお、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への対策に変更があり、船舶サイバーセキュリティ・レジリエンス計画書の内容に影響する変更がある場合は、船舶サイバーセキュリティ・レジリエンス計画書をアップデートする必要があります。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.3(3)(d) iv) 2)

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，すなわち次の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デバイスの使用手順が守られていること。
- アクセス制御ポリシー及び手順が守られていること。
- 物理的な保護が維持されていること。

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実施を証明するために、ウイルス，マルウェア，スパム及び悪意のあるコードへの対策に用いられるセキュリティゾーン境界デバイスについて、管理に関する記録又はその他の文書化された証拠として次のものを本会に提出する必要があります。

- 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デバイスの使用手順が守られていること。
- アクセス制御ポリシー及び手順が守られていること。
- 物理的な保護が維持されていること。

X 編 5.4.3(4) アクセス制御

■ 計画書に含めるべき内容

規則　X 編 5.4.3(4)(d) iv) 1)

船主は，少なくとも X 編 5 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（X 編 5.4.3(4)(c)i)）
– 訪船者のための物理的アクセス制御（X 編 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（X 編 5.4.3(4)(c)iii)）
– クレデンシャルの管理（X 編 5.4.3(4)(c)v)）
– 最小権限の原則（X 編 5.4.3(4)(c)vi)）

船舶サイバーセキュリティ・レジリエンス計画書に以下に関するアクセス制御方法を記載する必要があります。

- **物理的アクセス制御（X 編 5.4.3(4)(c)i)）**

分類 II 及び分類 III のコンピュータシステムは、通常時に施錠可能な部屋、管理されたスペース、施錠可能な棚等に備える必要があります。ただし、そのような場所、棚等は、船舶の安全な運航を妨げないよう、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ある必要があります。

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

主管庁、技術者、港湾関係者、船主等の訪船者が、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、例えば権限を与えられた管理者の監督下でのみアクセスを許可すること等により、制限される必要があります。

- 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（X 編 5.4.3(4)(c)iii)）

分類 II 及び分類 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、権限を与えられた管理者の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る必要があります。訪船者から一時的な接続（例えば文書印刷）を求められた場合には、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る必要があります。なお、ここでいう「物理的に阻止」とは、人員の立入り等を阻止することを示します。

– クレデンシャルの管理（X 編 5.4.3(4)(c)v)）

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）と共に保護される必要があります。アクセス制御一覧表とは、アクセス可否の設定をリストとして列挙したものであり、あるコンピュータシステムに対して、誰からのどの操作を許可するかが列挙されています。船上及び陸上の人員のアカウントは、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、不要になった際には削除される必要があります。
2) コンピュータシステムはアクセス制御により保護されていると同時に，当該コンピュータシステムの本来の機能に悪影響を与えないよう配慮する必要があります。また、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、強力なパスワード又は多要素認証を用いて保護してください。
3) 管理者特権は、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可能となるよう管理する必要があります。

– 最小権限の原則（X 編 5.4.3(4)(c)vi)）

1) 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全てのユーザーには，その職務の実施に必要な最小権限のみが与えられる必要があります。
2) 全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、可能な限り低い権限とする必要があります。例えば、1 回限り使用可能なクレデンシャル（ID、パスワード等）で得られる期間限定の権限を用いることが有効です。時間とともに権限が蓄積してしまうことは、例えばユーザーのアカウントを定期的に監査すること等により，回避されるべきです。

規則　X 編 5.4.3(4)(d) iv) 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（X 編 5.4.2(1)(c)）

– 権限を与えられた人員に許可される情報（X 編 5.4.3(4)(c)）
– 無線ネットワークで送信される情報（X 編 5.4.3(5)(c)）

船舶サイバーセキュリティ・レジリエンス計画書に以下に関する機密情報の管理方法を記載する必要があります。

- 機密情報（X 編 5.4.2(1)(c)）

機密情報（例えば、IP アドレス、プロトコル、ポート番号）へのアクセスを、権限を与えられた者だけに限定する必要があります。

- 権限を与えられた人員に許可される情報（X 編 5.4.3(4)(c)）

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、権限を与えられた人員に対してのみ許可される必要があります。

- 無線ネットワークで送信される情報（X 編 5.4.3(5)(c)）

1) 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、暗号化される必要があります。
2) 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ある必要があります。（すなわち、両用であってはならない。）
3) 無線ネットワークは、X編5.4.3(1)「セキュリティゾーン及びネットワークセグメント」に従って分離されたセグメントとして設計され，X 編 5.4.3(2)「ネットワークを防御する防護策」に従って防御されたものである必要があります。
4) 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る必要があります。
5) 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全てのユーザー（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ある必要があります。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.3(4)(d) iv) 3)

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。

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実施を証明するために、あらゆるアクセス制限に関して、管理に関する記録又はその他の文書化された証拠として次のものを本会に提出する必要があります。

- 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。

X 編 5.4.3(5) 無線通信

規則　X 編 5.4.3(2)(d) iv)

特筆した記載事項なし。

X 編 5.4.3(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

セキュリティリスクの高い，遠隔アクセス制御及び信頼できないネットワークとの通信において，それぞれより厳重な対策を施すための要件となります。

■ 計画書に含めるべき内容

規則　X 編 5.4.3(6)(d) i)

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おいて，遠隔アクセス及び信頼できないネットワークとの又は信頼できないネットワークを介した通信の管理について記述し，本章において少なくとも以下の要件に適合しなければならない。

- ユーザーマニュアル（5.4.3(6)(c)）
- 役割と権限（5.4.3(6)(c)）
- パッチとアップデート（5.4.3(6)(c)iii)2)）
- 遠隔ソフトウェアアップデートを行う前の確認（5.4.3(6)(c)iii)2)）

- 中断，中止，ロールバック（5.4.3(6)(c)iii)2)）

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おいて，遠隔アクセス及び信頼できないネットワークとの又は信頼できないネットワークを介した通信の管理について記述し，本章において少なくとも以下の要件に適合しなければならない。

本項目について、遠隔アクセスを行うデバイスを明示し、それぞれに対して適切な対策が取られていることを確認するため、下記の要件があります。

- **ユーザーマニュアル（5.4.3(6)(c)）**

遠隔接続のためには、5.4.3(6)(c)i)に記載されている通り、遠隔接続に関するユーザーマニュアルが作成される必要があります。本ユーザーマニュアルには下記の情報を記載する必要があります。

- **遠隔アクセスの方法**
- **遠隔アクセスに関する監査記録の確認方法**

サイバーセキュリティデザインの説明における、造船所の記載事項については本ガイドライン 4 章の 4 節、防御の第 6 項「5.4.3(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」をご覧ください。

4-3. サイバーセキュリティデザインの説明

X 編 5.4.3(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　P. 40

本マニュアルは、遠隔接続が可能な各デバイスを供給する供給者によって作成された書類を参考にすることができます。

- **役割と権限（5.4.3(6)(c)）**

遠隔接続のためには、5.4.3(6)(c)i)に記載されている通り、遠隔接続における役割と権限を明らかにしたガイドラインを作成する必要があります。遠隔接続に際しては、本ガイドライン 4 章の 4 節および 7 節の第 6 項「5.4.3(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」に関する説明にある通り、権限を持った船上の乗組員により遠隔接続が許可され、権限者により中断可能でなければなりません。

このガイドラインはユーザーマニュアルの一部として作成することでも差し支えありません。

4-3. サイバーセキュリティデザインの説明

X 編 5.4.3(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　P. 40

4-6. 船舶サイバーレジリエンス試験要領書

X 編 5.4.3(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　P. 63

そのため、実業務において遠隔接続を実施する人員を含めて、遠隔接続に関する役割と

権限は明らかにされている必要があります。

- パッチとアップデート（5.4.3(6)(c)iii）2)）

遠隔接続によってシステムのセキュリティパッチの供給やソフトウェアのアップデートを行う場合には、5.4.3(6)(c)iii) 2)にある通り、以下に示す追加の要件として、パッチ及びソフトウェアアップデートが効果的であること、またこれらを実施したことによって副次的な影響やサイバーインシデントを引き起こさないことを実証するための試験と評価を実施する必要があります。このような試験と評価については供給者によって確認報告書が作成されるので、アップデートに先立ってそれを入手し確認することが求められます。

そのような追加の要件に当てはまるデバイスを明らかにするため、それらのソフトウェアに関してはそのことを明らかにするための文書(一覧等)が作成される必要があります。

- 遠隔ソフトウェアアップデートを行う前の確認（5.4.3(6)(c)iii）2)）

遠隔接続によりセキュリティパッチの適用やソフトウェアのアップデートを実施する場合には、デバイスのソフトウェアをアップデートしたことで許容できない脆弱性が発生してしまうと、現地でのアップデートと比較して大きな悪影響をもたらします。そのため、遠隔の場合には特にアップデートによる影響は事前に確認される必要があります。そのため、遠隔接続によるセキュリティパッチの適用やソフトウェアアップデートの前には供給者からのアップデート情報を十分に理解し、アップデートを実施するかどうかを判断しする必要があり、その記録はアップデートのたびに文書化して残される必要があります。

- 中断，中止，ロールバック（5.4.3(6)(c)iii）2)）

ソフトウェアの遠隔保守によって不具合が出た場合や中断する必要のある場合には、安全に保守を中断し、元の状態に復旧できるようになっている必要があります。そのため、遠隔あるいは船上の認証された人員による作業の中断、および遠隔保守以前の状態にソフトウェアを復旧する機能が必要です。

船舶サイバーセキュリティ・レジリエンス計画書においては、このときの中断の方法と、復旧する手段を記載する必要があります。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.3(6)(d) iv) 2)

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，すなわち次の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，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，変更手順の管理に従って，供給者と協力して実施されていること。

- **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，実施されていること。**

本要求は、前節「計画書に含めるべき内容」の「ユーザーマニュアル（5.4.3(6)(c)）」に記載の通り、遠隔アクセスセッションが行われた際に、接続先や接続時刻などの必要な情報が記録される必要があることを述べています。これらの情報は遠隔アクセスの際に必ず記録する必要があり、年次検査の提出資料となります。

なお、これらの情報は機器の機能によりログとして記録されているため、年次検査ではそれらを文書化して提出することとなります。

- **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，変更手順の管理に従って，供給者と協力して実施されていること。**

本要求は、前節「計画書に含めるべき内容」の「遠隔ソフトウェアアップデートを行う前の確認（5.4.3(6)(c)iii）2)）」に記載されている、遠隔ソフトウェアアップデートの際に記録された文書の提示を要求するものです。これらの情報は遠隔保守が行われた際に必ず記録する必要があり、年次検査の提出資料となります。

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用

■ 計画書に含めるべき内容

規則　X 編 5.4.3(7)(d) iv) 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)）

携帯用又は可搬式デバイス経由のマルウェア感染によって、コンピュータシステムが障害を起こすことが一般的に知られています。そのため、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す。

船舶サイバーセキュリティ・レジリエンス計画書には、携帯用及び可搬式デバイスに関して以下の内容を記載する必要があります。

- **ポリシー及び手順（5.4.3(4)(c)iv）)**

携帯用及び可搬式デバイスの使用に関して、船主等により取り決められているポリシーを文書化し、船舶サイバーセキュリティ・レジリエンス計画書に記載する必要があります。

なお、当該ポリシーは、X 編 **5.4.3(4)(c)iv**）に従い、以下の事項を含めていただく必要があります。

- 可搬式デバイスのマルウェアについての確認手順並びに/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手順
- 船舶システムへのファイルのアップデート若しくは船舶システムからのデータのダウンロードに先立つデバイスのスキャン手順

また、可能であれば、上記に加えて鋼船規則 X 編表 X4.1 中 10 に規定する「可搬式及び携帯用デバイスの使用の管理」に関するメーカーの推奨事項も含めてください。

- 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)）

X 編表 X4.1 中 10 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、未使用のインターフェースのポートは鍵付きのポートブロッカー等の物理的手段により保護される必要があります。その手段や方法について記載してください。

なお、物理的手段によるインターフェースのポートの保護が必要となるものに関する情報については、サイバーセキュリティデザインの説明に記載されています。

- 権限を与えられた人員による使用（5.4.3(7)(c)）

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となるように管理されなければなりません。そのため、計画書には以下の内容を記載してください。

- システムやデバイスごとに割り当てられた権限者
- 物理的アクセス制御を採用する場合は、鍵の管理方法
- ユーザー認証等による管理

- 許可されたデバイスのみの接続（5.4.3(7)(c)）

コンピュータシステムへの接続は、デバイス制御等によって、許可されたデバイスのみが可能となるように管理される必要があります。

コンピュータシステムに接続可能なデバイスを制限する方法等について記載してください。また、可能であれば、コンピュータシステムへの接続が許可されているデバイスの一覧についても記載してください。

- マルウェアの侵入についてのリスクの考慮（5.4.3(7)(c)）

携帯用及び可搬式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ポリシーに従う必要があります。船舶サイバーセキュリティ・レジリエンス計画書へのポリシー等の記載については、マルウェアの侵入のリスクを考慮した内容を含めてください。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.3(7)(d) iv) 2)

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。**

- 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。

携帯用及び可搬式デバイスの使用は、限られた人員のみに制限されなければなりません。当該デバイスの使用者及び使用日時等が分かる記録やその他文書化された証拠を、年次検査の際に提出資料として本会に提出してください。

また、当該デバイスが、その使用に関したポリシー及び手順（X 編 5.4.3(4)(c)iv）に従って使用されていることを示す証拠、例えば、マルウェアスキャン実施時のログファイルやデジタル署名等によるソフトウェアの正当性の確認の実施記録等についても文書化し、年次検査の際に提出資料として本会に提出していただく必要があります。

- 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。

コンピュータシステムに接続されているデバイスが、許可されたもののみであることを証明するアクセスログ等の記録を文書化したものを、年次検査の際に提出資料として本会に提出していただく必要があります。

- 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。

携帯用及び可搬式デバイスの物理的なインターフェースのポートは、物理的な不正アクセスを防ぐためにその使用が制限されなければなりません。ポートの使用を制限する手段が、「サイバーセキュリティデザインの説明」等の承認された設計書類に従って実装されていることを証明する証拠、例えば、ポートブロッカー等により保護されているポートの写真等を文書化し、年次検査の際に提出資料として本会に提出していただく必要があります。

検知

X 編 5.4.4(1) ネットワーク動作の監視

■ 計画書に含めるべき内容

規則　X 編 5.4.4(1)(d) iv) 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)）

- 異常な活動を明らかにし、認識すること（5.4.4）

本項は、運用段階におけるサイバー攻撃に関する兆候の早期発見を目的としています。

セキュリティ上の異常な事象を認知する手段を確立させることで、セキュリティインシデントの発生を早期に検出して対応までの期間を最短化し、被害を最小化することができます。具体的には、各コンピューターシステムのセキュリティ機能による監査記録を確認した際に異常な事象を発見する基準を明確化することが求められます。本目的を達成する手段として、異常な状態と正常の状態とを比較するために、監査対象となるシステムにおいて、通常運航時に想定される監査記録の標準的なトラフィック量および通信先を記載しておくといったことが挙げられます。

- セキュリティ監査記録の審査（5.4.4(1)(c)）

本項は、サイバー攻撃に関する兆候の早期発見、脆弱性の分析を目的としています。

上記の基準に従って定期的な監査ログの分析を行うことで、活動の履歴から異常活動を発見し、サイバー攻撃の兆候となる異常な活動を早期に発見することができます。また、監査ログの分析を通じてシステムセキュリティ機能のうちで脆弱性のある項目の発見にもつなげることができます。脆弱性が発見できれば、ログ情報をもとに適切な対策を検討することにつながります。

- インシデントを検出するための指示又は手順（5.4.5(1)(a)）

本項は、検知された事象がインシデントに相当するかどうかを早期に判断することを目的としています。

セキュリティ上の異常な事象を発見した場合でも誤検知の可能性はあり、攻撃の種類によって対応方法が変わります。そのため、あらかじめセキュリティ上の異常事象が発見された際の対応方法を定めておくことが求められます。具体的な手段としては、上述したセキュリティ機能による警報が発報された場合に、警報を把握すべき時期や人員の他、イ

ンシデントであると想定される事象の基準や正常と判断すべき事象の基準を定めておくことが挙げられます。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.4(1)(d) iv) 2)

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。

- **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。**

本項は、サイバー攻撃に関する兆候の早期発見、脆弱性の分析を目的としています。

本要件は検知に関して定期的な実施が求められる顕著なものです。具体的には、船舶の運用者は初回の年次検査までに記録された異常な事象のサンプルと、定期的なセキュリティ監査記録の検査計画およびその記録、インシデントと判断された事象があればその記録を本会に提示する必要があります。

X 編 5.4.4(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

■ 計画書に含めるべき内容

規則　X 編 5.4.4(2)(d) iv) 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)）

-

- **試験及び保守期間（5.4.4(2)(c)）**

本項は、X 編 4 章が適用となる各製品において、X 編 4 章表 X4.1 の「19. セキュリティ機能の検証」に基づく検証を定期的に行う必要があることを述べています。この検証の計画はサイバーセキュリティ・レジリエンス計画書に記載され、それに基づき検証された結果は文書化された記録として残される必要があります。

ここでは、通常の運航状況において本要件で要求される検証と診断機能を用いて試験と保守を行う時期を定めておくことを要求しています。これにより、定期的にセキュリティ機能の健全性を確認し、セキュリティ機能の有効性を常に保つことができます。

なお、これらの試験と保守の時期はコンポーネントのネットワーク上の重要度を考慮する必要があります。そのため、例えばファイアウォールなどのリスクの高い機器の検証頻度には留意してください。また、試験や保守に関わる人員についてはOT環境への理解が深い人員を配置するようにしてください。

関連するX編4章の要求については、「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ガイドライン（第1.0版）」のP101「19. セキュリティ機能の検証」をご覧ください。

- 定期的な保守（2.2.3-5(9)）

本項は、本会の定期検査で確認する内容を定めておくことを要求しています。

定期検査では、船舶サイバーレジリエンス試験手順書に基づく船級立会試験を実施する必要があります（2.2.3-5(9)を参照）。本試験におけるセキュリティ機能の検証に際して本要件に基づくセキュリティ機能の検証がどの範囲をカバーしているのかを明らかにする必要があります。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X編 5.4.4(2)(d) iv) 2)

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。

- 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。

本項は、セキュリティ機能の健全性を維持していることが日常的に試験されているかどうか確認するための項目です。

前項（5.4.4(2)(d)(iv)(1)）の運用段階に対する要求「試験及び保守期間（5.4.4(2)(c)）」に基づく試験と保守が行われていることを確認するため、その記録を本会に開示する必要があります。

対応

X編 5.4.5(1) インシデント対応計画書

■ 計画書に含めるべき内容

規則　X 編 5.4.5(1)(d) iv) 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，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

本項は，船舶サイバーセキュリティ・レジリエンス計画書に含まれる、インシデント対応計画書に記載すべき情報を明確化することを目的としています。

- **規則 X 編 5.4.5(1)（本要件）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**

本項は、サイバーインシデント発生時に、船上における責任者が各人員に指示を出し、迅速かつ正確にサイバーインシデントに対応できるように、それらの情報をインシデント対応計画書に含むことを目的としています。各人員が、それぞれの役割を迅速かつ正確に果たすことで、被害を最小限にとどめることができます。

- **規則 X 編 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**

本項は、サイバーインシデント発生時の、機側／手動制御への切替えに関する手順又は指示をインシデント対応計画書に含むことを目的としています。機側／手動制御に関する手順又は指示とは、例えば、機関遠隔制御装置に対するサイバーインシデントの発生を検知した際には、機関長が機関を機側制御に切替え、機関士 A に機関の機側制御を指示すること等です。

- **規則 X 編 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**

本項は、サイバーインシデント発生時に、船上における責任者が各人員に指示を出し、迅速かつ正確にセキュリティゾーンを隔離できるように、それらの情報をインシデント対応計画書に含むことを目的としています。セキュリティゾーンの隔離に関する手順又は指示とは、例えば、自動衝突予防援助装置（ARPA）に対するサイバーインシデントの発生を検知した際には、船長が船員 A に、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ことを指示する等です。

- **規則 X 編 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

本項は、サイバーインシデント発生時に、コンピュータシステムがいかにして安全な状態に達するかに関する情報を、インシデント対応計画書に含むことを目的としています。コンピュータシステムがいかにして安全な状態に達するかに関する情報とは、例えば、機関制御装置に対するサイバーインシデントの発生を検知した際、機関制御装置は自動的に出力 0（入出港中）又は船速 10knot（外洋航行中）となるように機関を制御する等です。

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.5(1)(d) iv) 2)

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。

本項は、船舶サイバーセキュリティ・レジリエンス計画書に含まれるインシデント対応計画書に記載されている内容が、継続的に実施されているかどうかを確認するための項目です。

- **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。**

インシデント対応計画書を責任者が継続的に管理していることが分かる、文書化された証拠を作成してください。

- **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。**

機側／手動制御に関する手順書又は指示書を責任者が継続的に管理していることが分かる、文書化された証拠を作成してください。

- **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。**

セキュリティゾーンの切断／隔離に関する手順書又は指示書を責任者が継続的に管理していることが分かる、文書化された証拠を作成してください。

- **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。**

発生したサイバーインシデントの一覧及びその対応記録を作成してください。

X 編 5.4.5(2) 機側、独立及び／又は手動の操作

規則　X 編 5.4.5(2)(d) iv)

特筆すべき事項なし。

X 編 5.4.5(3) ネットワークの隔離

規則　X 編 5.4.5(3)(d) iv)

特筆すべき事項なし。

X 編 5.4.5(4) ミニマルリスクコンディションへのフォールバック

規則　X 編 5.4.5(4)(d) iv)

特筆すべき事項なし。

復旧

X 編 5.4.6(1) 復旧計画書

■ 計画書に含めるべき内容

規則　X 編 5.4.6(1)(d) iv)

インシデント復旧計画として以下を記述すること。

- 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の説明。
- 5.4.6(2)に規定する要件に従った，バックアップの頻度，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可用性，ベンダーのサポート体制並びにコンピュータシステムの重要性。
- 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。

復旧計画書とは、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

トによる混乱又は故障の後、使用可能な状態へ復元するための計画書です。

具体的には、本要件中に含まれる要件の詳細（X 編 5.4.6(1)(c)iv）に示される以下の 6 つの情報について、計画書に含めるか、または参照するものとする必要があります。

1) 冗長の，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) バックアップ及び情報の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) システムのサポート業者，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

上記の情報を計画書に含めたうえで、以下の要件を満足いただく必要があります。

- **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の説明**

ここでは、前述 1)に示されるシステムの復旧手順について、船上の人員の役割と手順を明確にすることが求められます。

- **5.4.6(2)に規定する要件に従った，バックアップの頻度，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可用性，ベンダーのサポート体制並びにコンピュータシステムの重要性**

ここでは、各コンピュータシステム及びネットワークにおけるバックアップ及び復元の機能について、以下に掲げる事項を当該計画書へ含める必要があります。

バックアップの頻度：

供給者が示す各コンピュータシステムのバックアップの推奨頻度に基づいて、バックアップ計画を立案にすることが求められます。

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：

システムを稼働している場合に許容可能なダウンタイムを確保したうえで、バックアップの保守及び試験を行います。

制御のための代替手段の可用性：

各コンピュータシステム及びネットワークのバックアップの保守及び試験を実施する場合における代替手段の利用方法を示すことが求められます。

ベンダーのサポート体制：

各コンピュータシステム及びネットワークのバックアップの保守及び試験について、供給者又は保守整備者のサポートについて示すことが求められます。

コンピュータシステムの重要性：

各コンピュータシステムが運航にとってどれだけ重要かを決定することが求められます。具体的には、複数のコンピュータシステムに対してサイバーインシデントが発生した場合の復旧活動の優先順位を決定することが挙げられます。

- **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**

　ここでは、供給者から提供される資料である「インシデントをサポートする情報」に記載される「バックアップ，シャットダウン，リセット，復元及び再起動」の手順を参照することが要求されます。

　統合者が「サイバーセキュリティデザインの説明」中に、各コンピュータシステムと情報が参照できる資料のリストを作成することが要求されているため、計画書の作成においては、当該リストを転記いただくこととなります。

表 4.7　コンピュータシステム及び復旧に関する情報が参照できる資料のリスト

コンピュータシステム	製品名称	関連する資料
主機制御システム	***	リカバリープラン（参照番号：***）

■ 継続的に作成されるべき記録又は文書化された証拠

規則　X 編 5.4.6(1)(d) iv) 2)

- インシデント復旧のための指示及び／又は手順が，船上の責任者に提供されること。
- 復旧に必要な機器，ツール，文書並びに／又は必要なソフトウェア及びデータが，船上の責任者に提供されること。
- 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，復元及び再起動のマニュアル及び手順は，船上の責任者が利用できること。

- **インシデント復旧のための指示及び／又は手順が，船上の責任者に提供されること。**

　復旧計画書に含まれるインシデント復旧のための指示や手順は、船上の責任者が利用できるように保管される必要があります。

- **復旧に必要な機器，ツール，文書並びに／又は必要なソフトウェア及びデータが，船上の責任者に提供されること。**

　インシデントからの復旧に必要なリソースを明示し、船上の責任者が迅速に対応できることが求められます。証明する記録又はその他の文書化された証拠は、一例として以下が挙げられます。

  - 機器・ツールリスト：復旧に必要な機器やツールの一覧とその保管場所を記載したリスト

- ソフトウェア・データリスト：復旧に必要なソフトウェア及びデータを記載したリスト

- **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。**

　データの損失を防ぐために、定期的かつ正確にバックアップが実施することが求められます。証明する記録又はその他の文書化された証拠は、一例として以下が挙げられます。

- バックアップ実施記録：定期的なバックアップスケジュールに基づいた実施記録。

- **シャットダウン，リセット，復元及び再起動のマニュアル及び手順は，船上の責任者が利用できること。**

　復旧計画書に含まれるシャットダウン，リセット，復元及び再起動のマニュアル及び手順は、船上の責任者が利用できるように保管される必要があります。

X 編 5.4.6(2) バックアップ及び復元の機能

規則　X 編 5.4.6(2)(d)iv)

特筆すべき事項なし。

X 編 5.4.6(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

規則　X 編 5.4.6(3)(d)iv)

特筆すべき事項なし。

5章　立会検査の解説

本章では、X 編 5 章（UR E26）に規定する立会検査に関する詳細を解説します。

X 編 5 章（UR E26）では、統合者及び船主による立会検査の実施が要求されています。

統合者は、設計および建造後の試運転段階で実施する「試運転段階での検査」が求められます。本検査では、ネットワーク及び各コンピュータシステムのセキュリティ機能の動作検証を行い、X 編 5 章（UR E26）の要件への適合を確認します。

船主は、定期的検査の検査時期に応じた立会検査を実施することが求められます。これらの検査では、ネットワーク及び各コンピュータシステムのセキュリティ機能の運用状況の実証及び／又は動作検証を行い、船舶が X 編 5 章（UR E26）の要件への適合を維持しているかを確認します。

図 5.1　X 編 5 章（UR E26）における立会検査

各立会検査の詳細は、次ページ以降に解説しております。

立会検査の要件

5-1. 試運転段階での検査　P. 105

5-2. 初回の年次検査　P. 108

5-3. 二回目以降の年次検査／中間検査　P. 110

5-4. 定期検査　P. 111

5-1. 試運転段階での検査

試運転段階での試験では、承認された「船舶サイバーレジリエンス試験要領書」に従ってネットワーク及び各コンピュータシステムのセキュリティ機能の動作検証を実施することが求められます。

まず本試験の各要件は、X 編 5.4 に規定する「試運転段階」の項目に規定されています。

規則　X 編 2.2.3-4.(2)(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。

*船舶サイバーレジリエンス試験要領書

これらの要件は、本試験における試験項目として、「船舶サイバーレジリエンス試験要領書」に含まれます。そのため、本ガイドラインでは、4 章「提出資料の解説」中「4-6. 船舶サイバーレジリエンス試験要領書」に各要件の解説を記述しておりますので、本試験における各要件の解説はそちらをご参照ください。

4-6. 船舶サイバーレジリエンス試験要領書　P. 54

X 編 5.4.2 識別

X 編 5.4.2(1) 船舶資産インベントリ　P. 57

X 編 5.4.3 防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント　P. 58

X 編 5.4.3(2) ネットワークを防御する防護策　P. 59

X 編 5.4.3(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　P. 61

X 編 5.4.3(4) アクセス制御　P. 62

X 編 5.4.3(5) 無線通信　P. 62

X 編 5.4.3(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　P. 63

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用　P. 66

X 編 5.4.4 検知

X 編 5.4.4(1) ネットワーク動作の監視 P. 67

X 編 5.4.4(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 P. 71

X 編 5.4.5 対応

X 編 5.4.5(2) 機側、独立及び／又は手動の操作 P. 72

X 編 5.4.5(3) ネットワークの隔離 P. 73

X 編 5.4.5(4) ミニマルリスクコンディションへのフォールバック P. 73

X 編 5.4.6 復旧

X 編 5.4.6(1) 復旧計画書 P. 74

X 編 5.4.6(2) バックアップ及び復元の機能 P. 74

X 編 5.4.6(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 P. 75

また、「試運転段階での検査」では、コンピュータシステムに関わる試験の省略について、以下のとおり規定されています。

規則　X 編 2.2.3-4.(2)(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。

X 編 5 章（UR E26）の適用範囲となるコンピュータシステムは、X 編 4 章（UR E27）に従って本会の承認を受ける必要があり、その中でコンピュータシステムのセキュリティ機能の確認試験を実施することとなります。試運転段階の試験では、いくらかの要件において、コンピュータシステムのセキュリティ機能の確認試験を実施することになりますが、これらの試験が X 編 4 章（UR E27）の承認プロセスを通して正常に実施されている場合、当該試験を省略することが可能です。

該当する試験を省略する場合、X 編 4 章（UR E27）により規定された該当するセキュリティ機能に関する試験結果を添付の上、機関部へお問い合わせいただくことになります。

5-2. 初回の年次検査

規則　X 編 2.2.4-5.(7)(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。

初回の年次検査では、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」に基づく運用状況を実証することが求められます。したがって、船主は、本計画書を実際に運用し、初回の年次検査までに記録書等の運用の証拠となる文書類を準備しておく必要があります。

本検査では、本会検査員が「船舶サイバーセキュリティ・レジリエンス計画書」に記載された通り記録書／証拠が作成・保管されていることを確認します。本ガイドラインでは、作成が必要となる記録または証拠として、4 章「提出資料の解説」中「4-7. 船舶サイバーセキュリティ・レジリエンス計画書」に詳しく解説しておりますので、本試験における各要件の解説はそちらをご参照ください。

4-7. 船舶サイバーセキュリティ・レジリエンス計画書　P. 76

X 編 5.4.2 識別

X 編 5.4.2(1) 船舶資産インベントリ　P. 79

X 編 5.4.3 防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント　P. 82

X 編 5.4.3(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　P. 84

X 編 5.4.3(4) アクセス制御　P. 86

X 編 5.4.3(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　P. 89

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用　P. 92

X 編 5.4.4 検知

X 編 5.4.4(1) ネットワーク動作の監視 P. 95

X 編 5.4.4(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 P. 96

X 編 5.4.5 対応

X 編 5.4.5(1) インシデント対応計画書 P. 97

X 編 5.4.6 復旧

X 編 5.4.6(1) 復旧計画書 P. 100

5-3. 2 回目以降の年次検査／中間検査

規則　X 編 2.2.3-5.(8)

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。

2 回目以降の年次検査／中間検査について解説します。まず、2 回目以降の年次検査と中間検査については、検査内容に違いはございません。その上で、本項にてまとめて解説します。

2 回目以降の年次検査／中間検査では、初回の年次検査同様、船舶サイバーセキュリティ・レジリエンス計画書に基づく運用状況を実証することが求められます。したがって、本計画書に基づき運用し、すべての記録書の作成を行う必要があります。ただし、初回の年次検査と異なる点としては、検査における記録書等の確認については、「本会の要請に応じて」としており、すべてではなくサンプリングとする場合があることです。ここでの判断は検査員に委ねられることが前提としたうえで、一般的には以下のような船舶ネットワークや当該計画書に前回検査から変更があるケースが考えられます。

・コンピュータシステムに変更があった場合

ソフトウェアのアップデートやハードウェアの構成要素の変更など、コンピュータシステムに変更があった場合、船舶サイバーセキュリティ・レジリエンス計画書に基づいた変更管理が実施されていることを確認します。

・船舶サイバーセキュリティ・レジリエンス計画書をアップデートした場合

運用の見直しにより、本計画書をアップデートした場合は、本会の再承認を受けたうえで、該当箇所の確認検査を実施します。

本ガイドラインでは、作成が必要となる記録または証拠として、4 章「提出資料の解説」中「4-7. 船舶サイバーセキュリティ・レジリエンス計画書」に詳しく解説しておりますので、本試験における各要件の解説はそちらをご参照ください。

4-7. 船舶サイバーセキュリティ・レジリエンス計画書　P. 76

5-4. 定期検査

規則　X 編 2.2.3-5.(9)

船主は，船舶の船級証書が更新された際に，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。

定期検査では、2 回目以降の年次検査／中間検査時に要求される検査に加えて、「船舶サイバーレジリエンス試験要領書」に従って、ネットワーク及び各コンピュータシステムのセキュリティ機能の動作検証を実施することが求められています。「船舶サイバーレジリエンス試験要領書」は、統合者によって作成され、試運転段階での試験を実施したうえで、船主へ引き渡される資料です。本試験における各要件は、本試験における試験項目として、本資料に含まれます。そのため、本ガイドラインでは、4 章「提出資料の解説」中「4-6. 船舶サイバーレジリエンス試験要領書」に各要件の解説を記述しておりますので、本試験における各要件の解説はそちらをご参照ください。

4-6. 船舶サイバーレジリエンス試験要領書　P. 54

・立会検査が必須の要件

X 編 5.4.2 識別

X 編 5.4.2(1) 船舶資産インベントリ　P. 57

X 編 5.4.3 防御

X 編 5.4.3(1) セキュリティゾーン及びネットワークセグメント　P. 58

X 編 5.4.3(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　P. 61

X 編 5.4.3(5) 無線通信　P. 62

X 編 5.4.3(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　P. 63

X 編 5.4.3(7) 携帯用及び可搬式デバイスの使用　P. 66

なお、本検査で要求されているいくつかの試験においては、「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」としています。したがって、コンピュータシステムが変更されていない場合には、該当する試験を省略することが原則可能です。立会検査の省略が可能な要件の一覧は以下のとおりです。

・立会検査の省略が可能な要件

X 編 5.4.3 防御

X 編 5.4.3(2) ネットワークを防御する防護策　P. 59

X 編 5.4.4 検知

X 編 5.4.4(1) ネットワーク動作の監視　P. 67

X 編 5.4.5 対応

X 編 5.4.5(2) 機側、独立及び／又は手動の操作　P. 72

X 編 5.4.5(3) ネットワークの隔離　P. 73

X 編 5.4.5(4) ミニマルリスクコンディションへのフォールバック　P. 73

X 編 5.4.6 復旧

X 編 5.4.6(2) バックアップ及び復元の機能　P. 74

X 編 5.4.6(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　P. 75

一般財団法人 日本海事協会

技術本部　機関部

〒102-0094　東京都千代田区紀尾井町 3 番 3 号
Tel：　03-5226-2022
E-mail：mcd@classnk.or.jp

www.classnk.or.jp

July 2024