

# 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）を作成し、最新版に維持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。

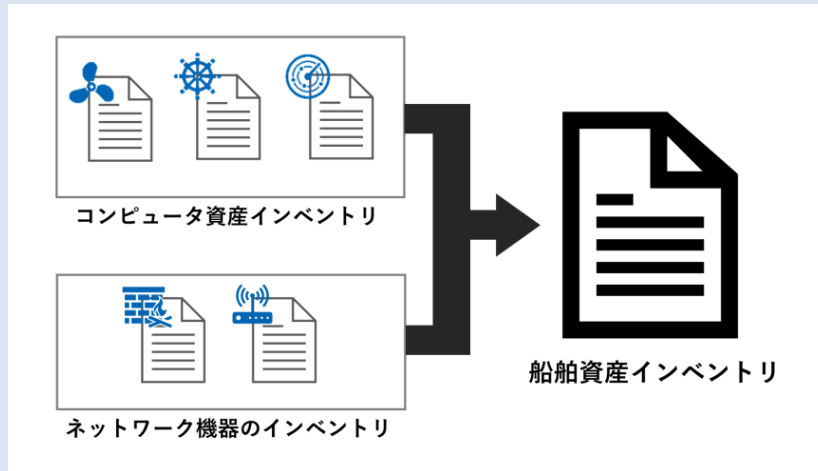


図 1.2 船舶資産インベントリ

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、さらに本船でのシステムの用途やインターフェースに関する情報などを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版に維持することで、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、サイバーインシデント発生時に迅速に対応することが可能です。
- コンピュータシステムの変更管理を行う際に参照することができる基礎資料になります。

### 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。

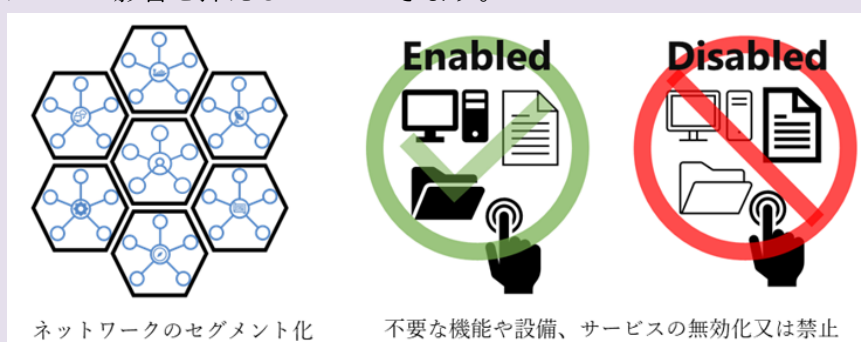




図 1.3 本要件で求められる特に重要な防護策

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における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、異常を認知することです。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監査記録（ログ）として記録すること、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、異常を特定できます。

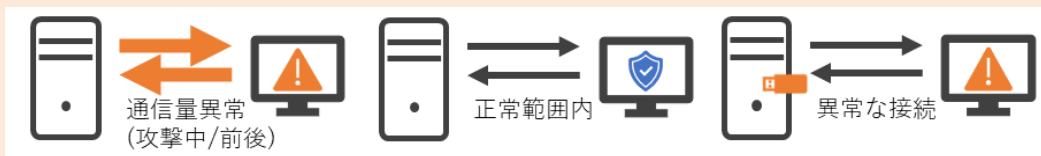


図 1.4 設計範囲外のネットワーク動作による警報

- **セキュリティ機能の検証**：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、実施時期を策定したうえで検証する必要があります。それにより船舶のセキュリティ機能を常に有効に維持することができます。

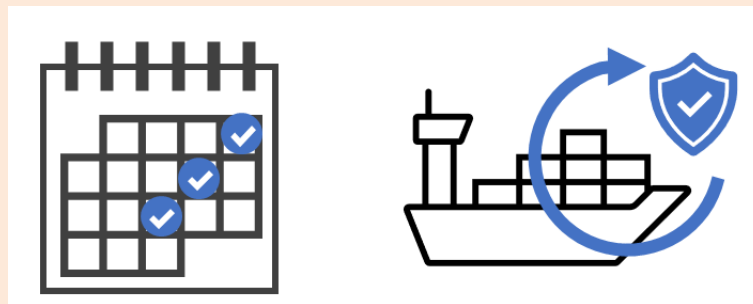


図 1.5 定期的なセキュリティ機能の検証による保護

### 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や発電システム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。

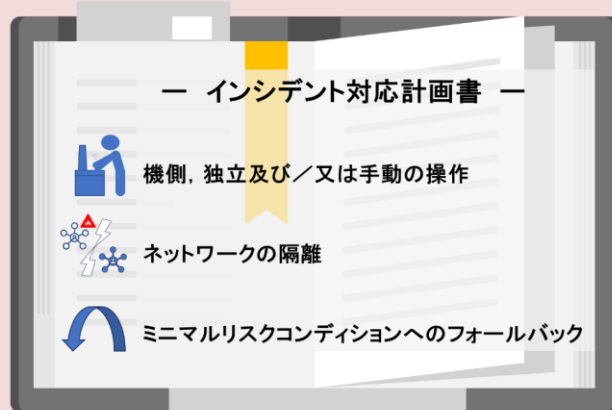




図 1.6 インシデント対応計画書

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ト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。

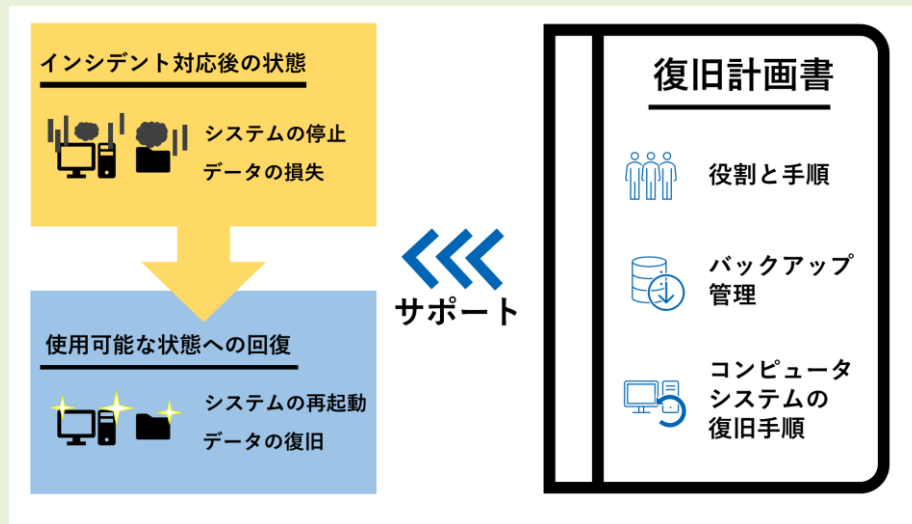




図 1.7 復旧計画書

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。