2024 ClassNK 技術セミナー

サイバーレジリエンス
UR E26, E27
に関する規則概要

8 October 2024 Tokyo, Japan

日本海事協会　機関部

背　景

従来の舶用システム　**物理的な接続や制御**に依存
サイバー空間との**接点なし**

近年の舶用システム　**コンピュータ**の使用
ネットワークを利用した**相互接続**

サイバー空間に晒されることで、**攻撃のリスクが増大**

サイバー攻撃による海運業界の平均被害額*

2022年　**18.2万ドル**

約3倍 ▶

2023年　**55万ドル**
(約8250万円)

ランサムウェアによる身代金要求回数*

過去12ヶ月で　4.5倍　(2023年10時点)
平均支払額　320万ドル

IACS UR E26　**船舶のサイバーレジリエンス**
IACS UR E27　**船上のシステム及び機器のサイバーレジリエンス**

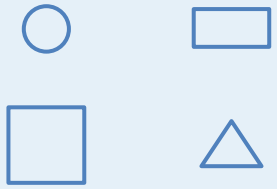
2024/7/1建造契約船から適用

*出典）2023年10月24日付日本海事新聞『サイバー攻撃、海運業界は「絶好の標的」。被害平均額55万ドルに急騰』より抜粋、海事調査機関セティウスの調査より

IACS UR E27 (Rev.1)

（鋼船規則X編4章）
「船上のシステム及び機器のサイバーレジリエンス」

メーカ（供給者）は、
サイバーレジリエンスを
考慮した機器を供給

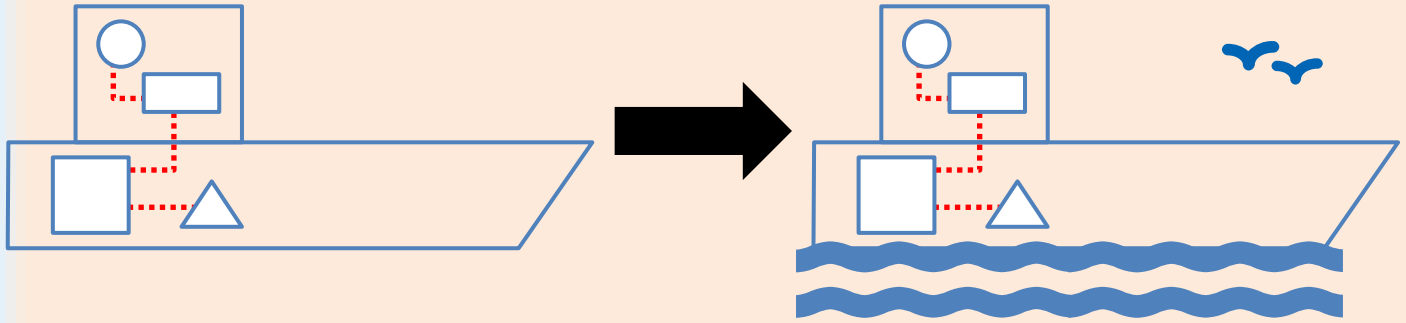


IACS UR E26 (Rev.1)

（鋼船規則X編5章）
「船舶のサイバーレジリエンス」

造船所（統合者）は、
サイバーレジリエンスを
確保した船舶を建造

船主は、
就航中の船舶の
サイバーレジリエンスを維持



サイバーレジリエンス

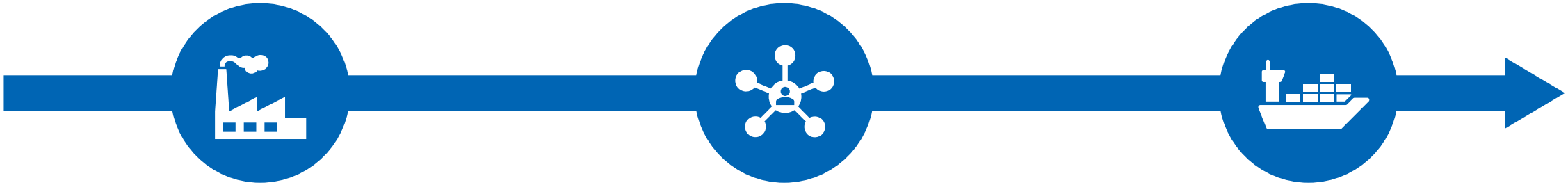
サイバー攻撃等によるサイバーインシデントの発生を低減し、影響を軽減し、発生した場合でも早期に復旧する機能

課題

本規則は**細部にわたり専門的な内容が多数**

例）ネットワークスイッチ、OTシステム、プロトコル、セグメント化、セキュリティゾーン……

さらに、**各ステークホルダーの対応が必要**



メーカ
機器の設計 / 製造

造船所
船舶の設計 / 建造

船主
船舶の運航

これらを踏まえ、NKでは規則への対応を支援

本会は対応支援のため、解説書となるガイドラインを発行済

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

X編4章 (UR E27)

対象　舶用機器メーカ

発行　2023年11月

内容　適用対象
承認プロセス
要件の説明
提出資料
立会試験
使用承認の説明
など

船舶のサイバーレジリエンスに関するガイドライン

X編5章 (UR E26)

対象　造船所
船主

発行　2024年7月

内容　適用対象の例示
ネットワーク構成
各要件の解説
提出資料
立会試験
適用除外
など

ポータルサイトに掲載中
https://www.classnk.or.jp/hp/ja/activities/cybersecurity/ur-e26e27.html

適用対象と範囲

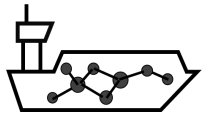
造船所における初期対応

適用対象船舶であるか判断

船舶のネットワーク構成を設計、
適用範囲に含まれるコンピュータシステムを特定

除外のための基準を満たす
一部の**コンピュータシステムを適用除外**

適用範囲の供給者にE27の承認取得を手配

適用対象船舶 

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

- 国際航海に従事する旅客船（高速旅客船を含む）
- **総トン数500トン以上の国際航海に従事する貨物船**
- 総トン数500トン以上の国際航海に従事する高速船
- 総トン数500トン以上の海洋資源掘削船
- 建設（例えば風力発電設備の設置、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）に従事する自航式海洋構造物

💡**内航船**や**総トン数500トン未満の貨物船**は**非強制**

適用対象と範囲

適用範囲に含まれるシステムと機器

適用対象のOTシステム	船舶の運航・制御に直接関わるシステム
適用対象のOTシステム以外の、適用対象のシステム	適用対象のOTシステムと同じセキュリティゾーンに存在するシステム
適用対象のシステムの通信を制御・管理するネットワーク機器	適用対象のシステムの通信を制御・管理するネットワーク機器
適用対象外のシステム	適用対象のOTシステムと同じセキュリティゾーンの外に存在するシステム


VDR・ECDISデータサーバ

適用範囲に含まれないシステムと機器

適用対象と範囲

ClassNK

適用対象のOTシステム	船舶の運航・制御に直接関わるシステム

- **推進**
- **操舵**
- **投錨**及び**係留**
- **発電**及び**分電**
- **火災探知**及び**消火システム**
- **ビルジ**、**バラストシステム**及び**積付計算機**
- **水密性**及び**浸水検知**
- **照明**（例えば、非常灯、航海灯等）

- **安全が要求されるシステム**であって、当該システムの混乱又は機能障害が船舶の運航にリスクをもたらしうるもの

  （例えば、緊急停止システム、荷役安全システム、圧力容器安全システム、ガス検知システム等）
- 条約により要求される**航海設備**
- 船級規則又は条約により要求される**船内及び船外通信システム**

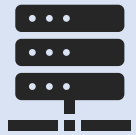
具体的なOTシステムについてはガイドラインで例示

適用範囲に含まれるシステムと機器

適用対象のシステムの通信を制御・管理するネットワーク機器

適用対象のシステムの通信を制御・管理するネットワーク機器

Firewall



ルータ

スイッチ

適用対象のOTシステム以外の、適用対象のシステム

適用対象のOTシステムと同じセキュリティゾーンに存在するシステム

適用対象のOTシステム

VDRデータサーバ

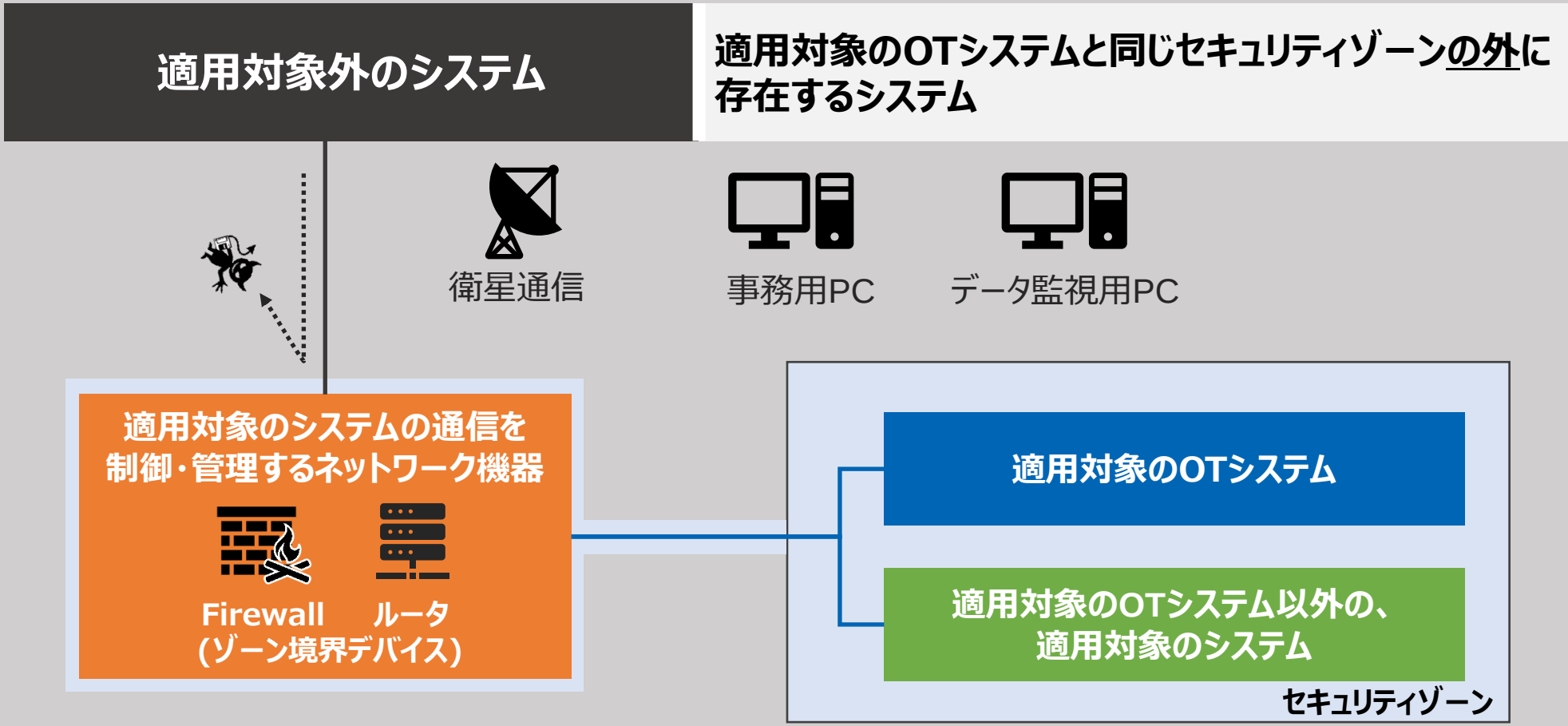
ECDISデータサーバ

同じセキュリティゾーンにあるシステム

セキュリティゾーン

適用範囲内のコンピュータシステムはX編4章(UR E27)の承認が必要

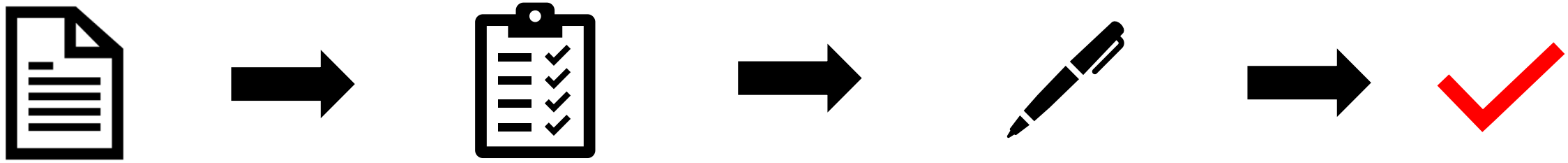
適用範囲に含まれないシステムと機器



セキュリティゾーン：ゾーン境界デバイスを境界とした、同等のセキュリティレベルを持つ機器の集合

適用対象と範囲

リスク評価による適用除外



適用除外とする機器をリスト化　「合格基準」を満たしているかチェック　「追加基準」についても考慮　適用除外

「合格基準」
（適用除外のために必須）

- IPネットワーク接続がない
- 全ての空きポートが使用できない
- 設置場所に物理的アクセス制御がされている
- 統合システムでない

「追加基準」
（適用除外のために考慮すべき）
完全に満たさなくても本会が適当と認める場合受け入れ可

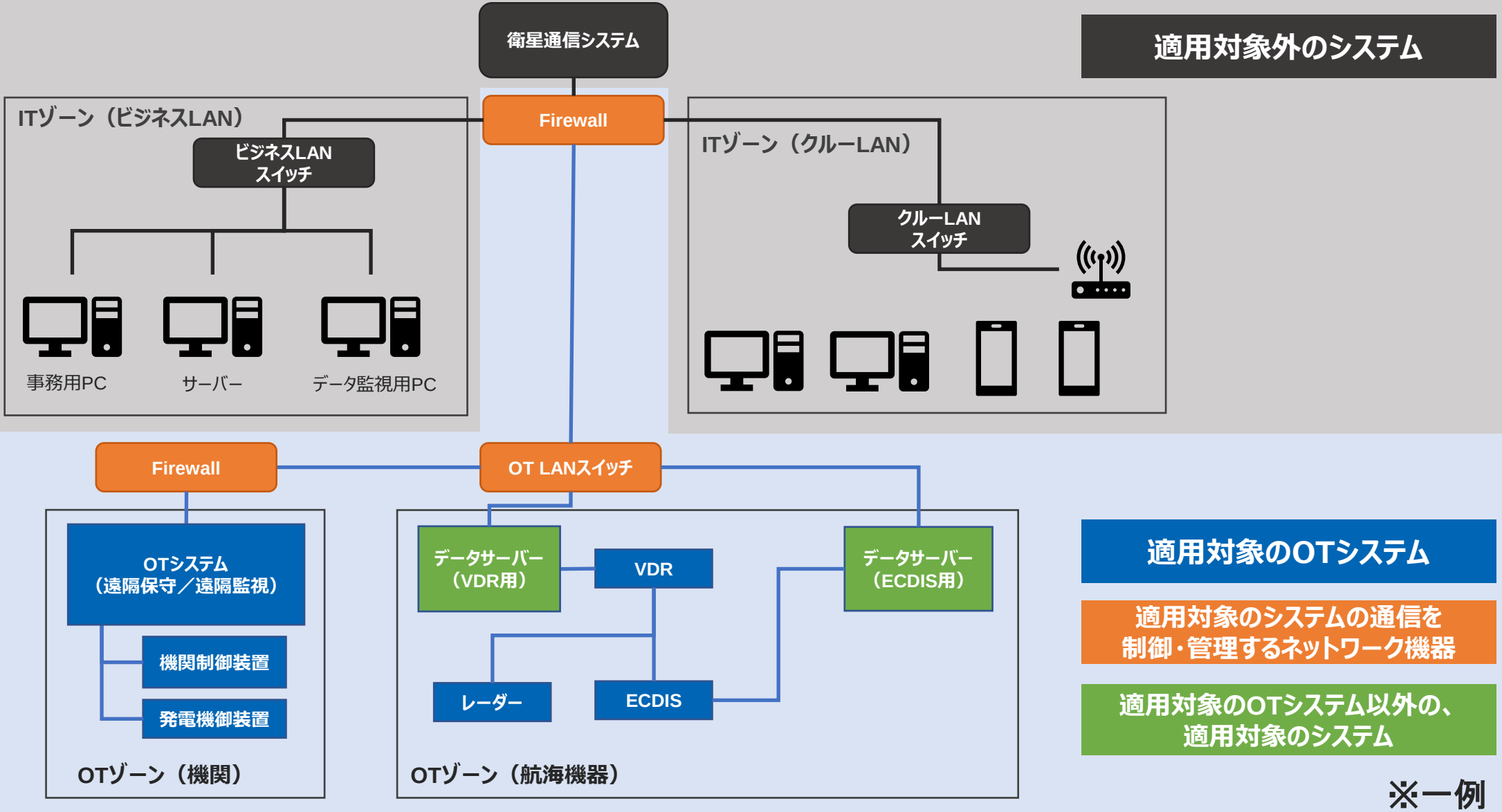
- 分類 III に該当しない
- 脆弱性，脅威，インシデントの影響へのリスク評価が適切
- 攻撃対象領域が最小化されている

- 適用対象範囲に含まれる機器であっても、リスク評価を実施することで適用対象外とすることが可能
- リスク評価は造船所が個船毎に実施（適用除外としたい機器に対してのみでOK）

適用対象と範囲

ClassNK

E26範囲外



適用対象外のシステム

適用対象のOTシステム

適用対象のシステムの通信を
制御・管理するネットワーク機器

適用対象のOTシステム以外の、
適用対象のシステム

※一例

E26範囲内

適用対象と範囲

造船所における初期対応

適用対象船舶であるか判断

船舶のネットワーク構成を設計、
適用範囲に含まれるコンピュータシステムを特定

除外のための基準を満たす
一部の**コンピュータシステムを適用除外**

適用範囲の供給者にE27の承認取得を手配

X編5章（UR E26）の要件概要

目 的　5つの要素の要件により、船舶のサイバーリスクを軽減し、回復力により安全運航を確保

内 容　UR E26では、船舶がサイバー攻撃などから守るために必要となる対策を、5つの要素に分解したうえで、各要件として設定

- **識別**　船上のシステムやネットワーク機器などの資産を**「見える化」**すること
- **防御**　起こりうるサイバーインシデントの**規模と頻度を最小化**すること
- **検知**　**サイバーインシデントを特定**すること
- **対応**　サイバーインシデントを検知した場合の**影響を最小化するための手段を構築**すること
- **復旧**　サイバーインシデントによる混乱又は故障の後、**使用可能な状態へ回復**すること

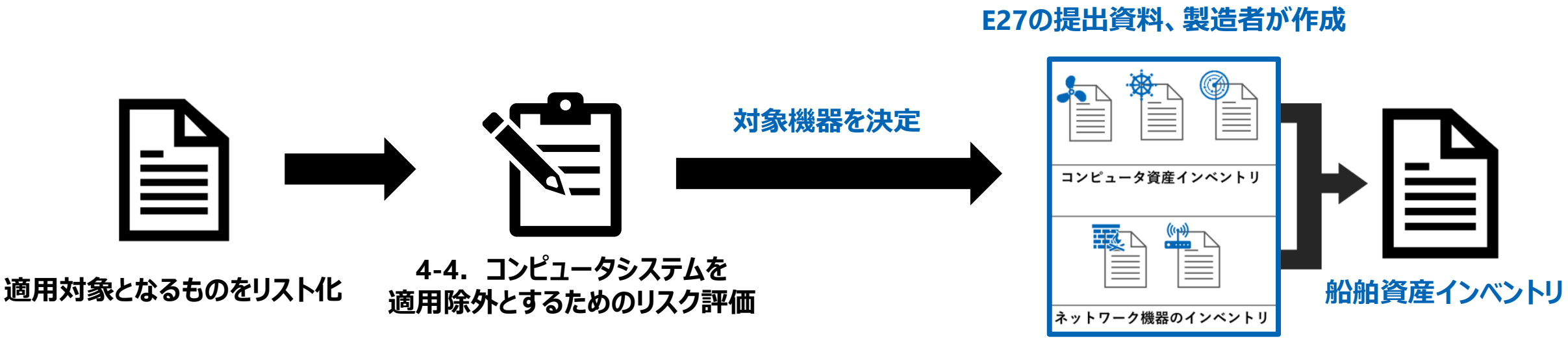
造船所の作成資料

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

船舶資産インベントリ

目的 船舶上のコンピュータシステムを一覧で把握可能とし、適切な対策を実施できるようにする

概要 船舶に搭載されるコンピュータシステム、ネットワーク機器、ソフトウェア等をリスト化したもの

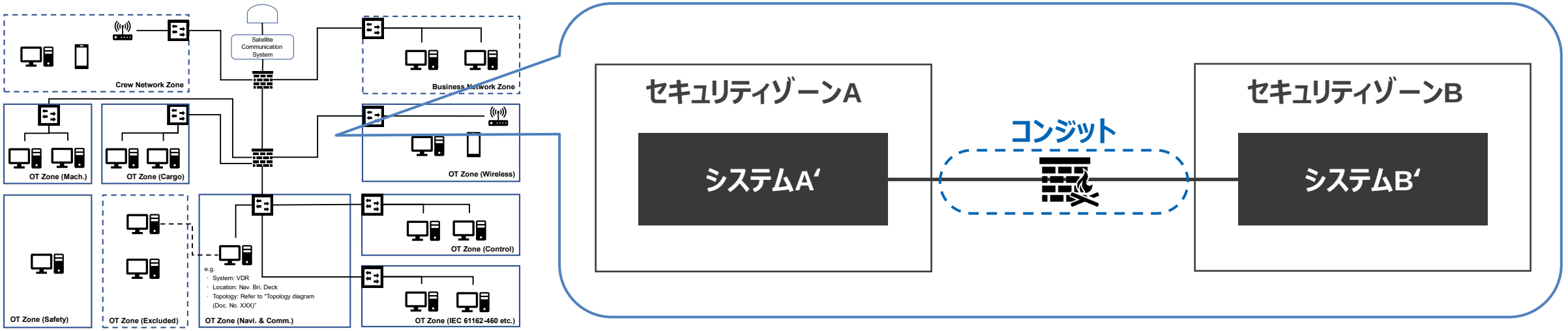


- ✓ 適用範囲に含まれるコンピュータシステムを全て記載する。**船主支給品**についても含めること。
- ✓ 設計の早期にNKに提出することを推奨。未定事項についてはその旨記載して提出する。ただし、試運転段階での検査までに最終化が必要。

ゾーン及びコンジット図

目的 船上のネットワーク構成を明確化し、適切な対策を実施できるようにする

概要 船上のネットワーク構成を視覚的に表現した図で、**セキュリティゾーン**（セキュリティレベルの異なる領域）と**コンジット**（ゾーン間の通信経路）の関係を示す

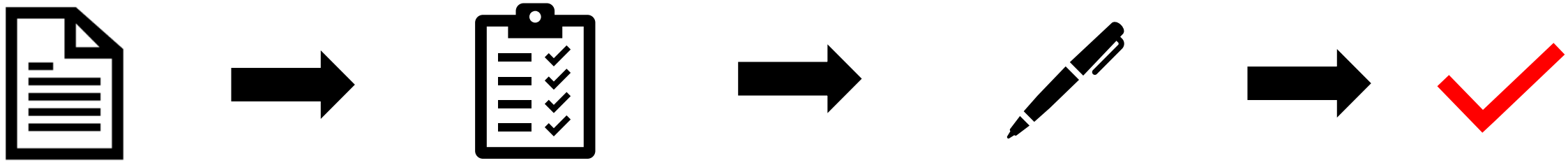


✓ ゾーン間の境界やコンジットにおけるセキュリティ対策を明確に示すこと。

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

目的 特定のコンピュータシステムの船舶に与えるサイバーリスクを評価、妥当である場合は適用範囲から除外することで、船舶全体のサイバーレジリエンスを合理的に管理する

概要 適用除外を希望するコンピュータシステムについて、除外が妥当であることを示すもの



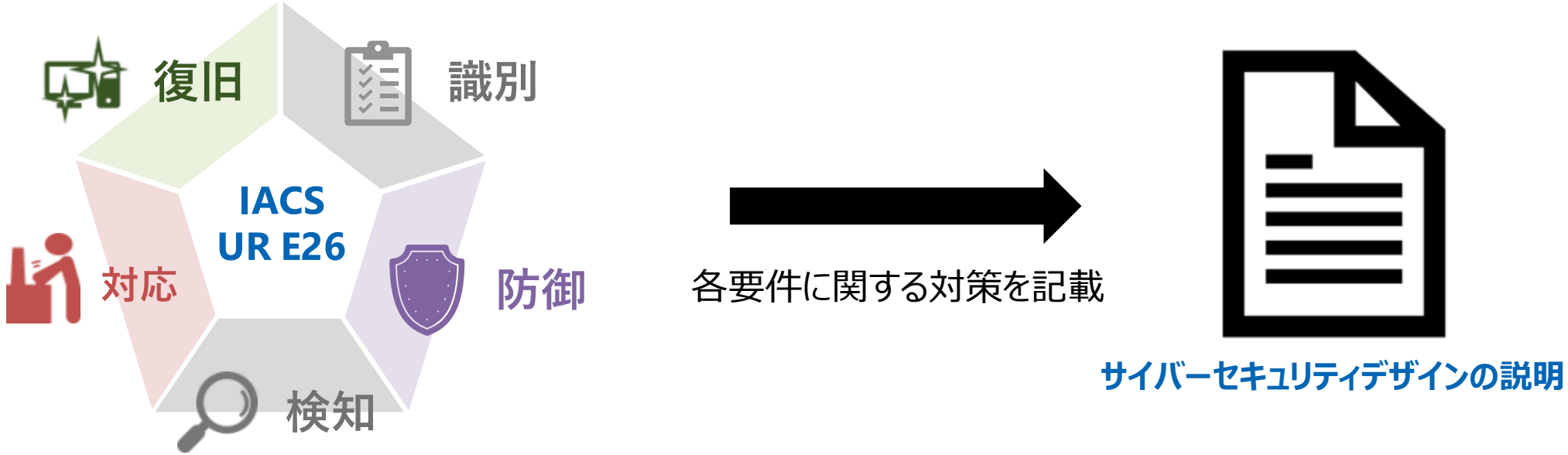
適用除外とする機器を抽出　4つの「合格基準」を満たしているか確認　3つの「追加基準」についても考慮　適用除外

- ✓ 3つの追加基準については、完全に満たさなくても本会が適当と認める場合受け入れ可能。
- ✓ 適用除外しないコンピュータシステムについては含めなくてよい。

サイバーセキュリティデザインの説明

目的 船舶のサイバーセキュリティ対策の設計思想と実装方法を明確化し、対策の有効性と妥当性を評価するための情報を提供する

概要 「防御」、「対応」、「復旧」の要件に関する技術的な対策をまとめたもの



✓ 船主が作成する「船舶サイバーセキュリティ・レジリエンス計画書」の作成に活用される

補完的対策の説明

目的 セキュリティ対策をどのように補完しているか説明し、その有効性と安全性を評価できるようにする

概要 X編4章 (UR E27) に規定するセキュリティ要件を満たすために採用する補完的対策をまとめた文書

- ✓ 補完的対策によりセキュリティ要件をみたしたコンピュータシステムを明確化。
- ✓ 補完対象のセキュリティ機能及びその補完的対策を説明。
- ✓ 必要に応じて各コンピュータシステムの「セキュリティ機能の説明」への参照情報。

船舶サイバーレジリエンス試験要領書

目的 船舶のサイバーセキュリティ対策が有効に機能することを確認するための試験手順の策定

概要 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を検証するための試験方案

・製品ごとの試験要領を集約
・ネットワークに関する内容を追加

船舶サイバーレジリエンス試験要領書

- ✓ 試験項目、試験方法、判定基準などを具体的に記載する
- ✓ 船舶建造中は統合者、就航後は船主により実施される立会い試験（定期検査・システム変更時）に利用

X編5章（UR E26）の要件概要

船主の作成資料

- 船舶サイバーセキュリティ・レジリエンス計画書

船舶サイバーセキュリティ・レジリエンス計画書

目的 船舶のサイバーセキュリティリスクを管理し、サイバー攻撃に対する回復力を確保することで、安全な運航を実現する。

概要 船舶のサイバーセキュリティリスクへの対応ポリシー、手順、体制などを具体的に示す計画書

各要件に関する計画を記載

変更管理、ファイアウォール管理、可搬式デバイス管理、インシデント対応計画、etc.

船舶サイバーセキュリティ・レジリエンス計画書

- ✓ 初回の年次検査までにNKへ提出が必要
- ✓ 定期検査や変更管理などの際に、計画書の内容の実施状況を証明する記録などのNK検査員への提示が必要

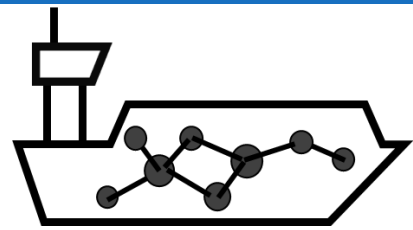
X編5章(UR E26)適合のためのプロセス

ClassNK

設計段階

引き渡し

運航段階



1 → 2 → 3 → 4

1 適用対象の特定 NKへの図面提出

造船所

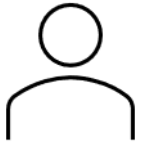
適用対象となるシステムを早期に特定し、発注時にはメーカに**4章承認**要否を伝達

各種提出図面を完成次第**提出**

船主

造船所の図面には**船主支給品**も含めるため、早期に情報を造船所に連絡

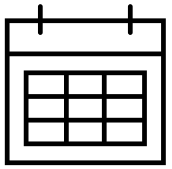
2 試運転段階の NK立会い検査



造船所

提出済みの資料
「船舶サイバーレジリエンス試験要領書」に基づき**立会検査**を実施

3 初回年次検査までの NKへの図書提出



船主

初回の年次検査までに
「船舶サイバーセキュリティ・レジリエンス計画書」を提出、**承認**を得る

年次検査では本計画書に基づく管理の**記録**を提出

4 NK年次・中間・定期検査

船主

年次・中間検査では、検査員の要求に応じて「船舶サイバーセキュリティ・レジリエンス計画書」に基づく**記録**を提示

定期検査では、
「船舶サイバーレジリエンス試験要領書」に基づき**立会検査**を実施

まとめ

- 適用対象と範囲は**ネットワーク構成で変化**
- 3つの資料は**早めに提出**(未決定項目は**その記載も可**)
  - 船舶資産インベントリ
  - ゾーン及びコンジット図
  - コンピュータシステムを適用除外とするためのリスク評価
- 造船所資料にも**船主支給品を記載**
- 船舶サイバーレジリエンス試験要領書に基づく**立会試験が必要**
- **初回の年次検査までに計画書の承認が必要**

for your kind attention