造船所殿向けご説明

船舶のサイバーレジリエンス

（鋼船規則X編5章 / UR E26 Rev.1）

2026年6月

日本海事協会　機関部

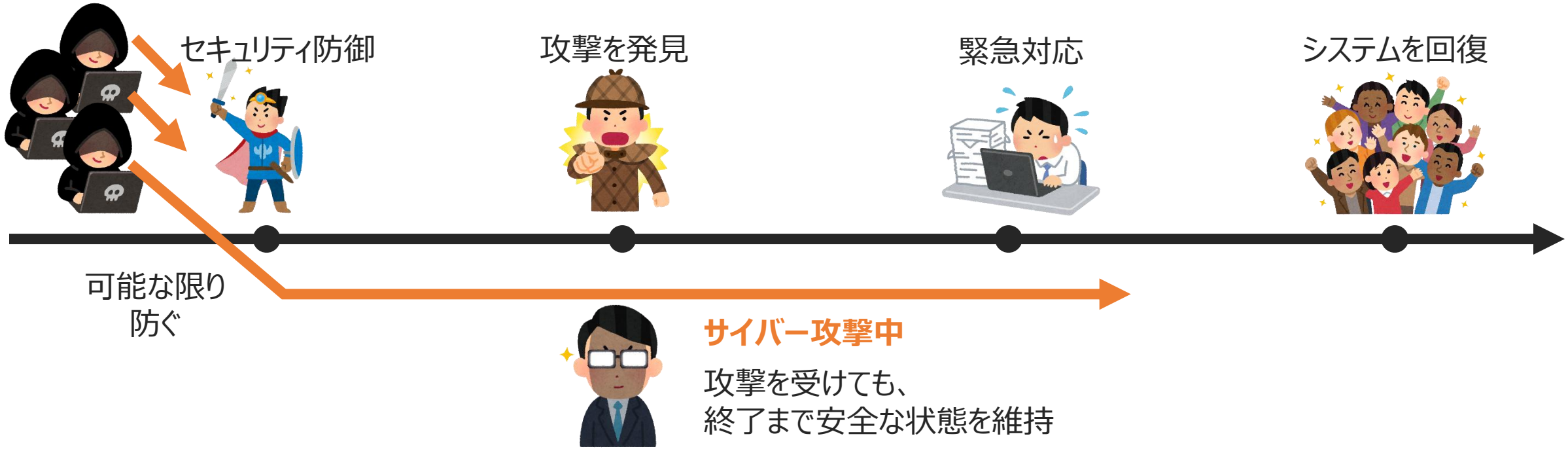
目次

サイバーレジリエンスとは？

サイバー攻撃等による被害である**サイバーインシデント**の発生を低減し、影響を軽減する機能

サイバーセキュリティ：サイバー攻撃を防ぐことに焦点

サイバーレジリエンス：攻撃を防げない場合の回復する力**「レジリエンス」**まで確保



各要件の詳細については、ガイドラインやFAQもご参考ください

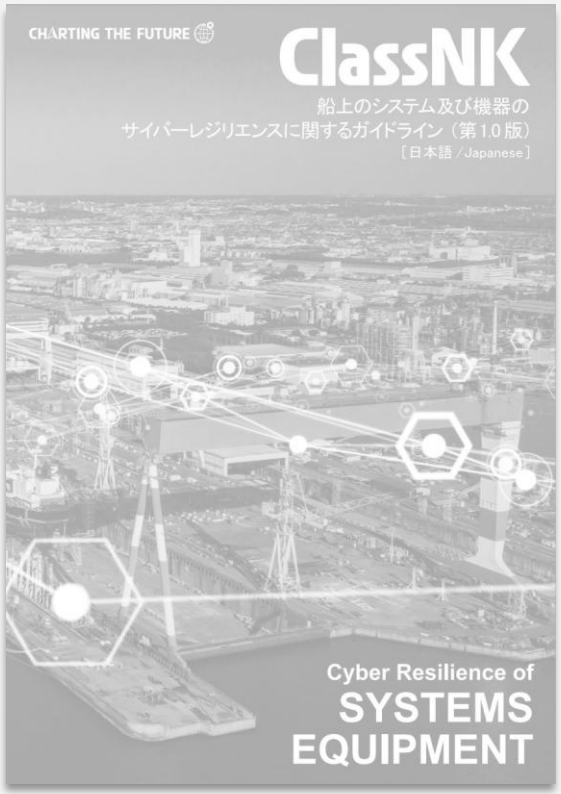
船上のシステム及び機器のサイバーレジリエンスに関するガイドライン

X編4章

対象　舶用機器メーカ

内容　適用対象
承認プロセス
要件の説明
提出資料
検査
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

対象　造船所
船主

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
検査
適用除外

など

🌐ポータルサイトにガイドライン、FAQ、解説動画を掲載中
https://www.classnk.or.jp/hp/ja/activities/cybersecurity/ur-e26e27.html

各段階で供給者、統合者、船主が役割を負う

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」

IACS UR E26

「船舶のサイバーレジリエンス」

メーカ（供給者）

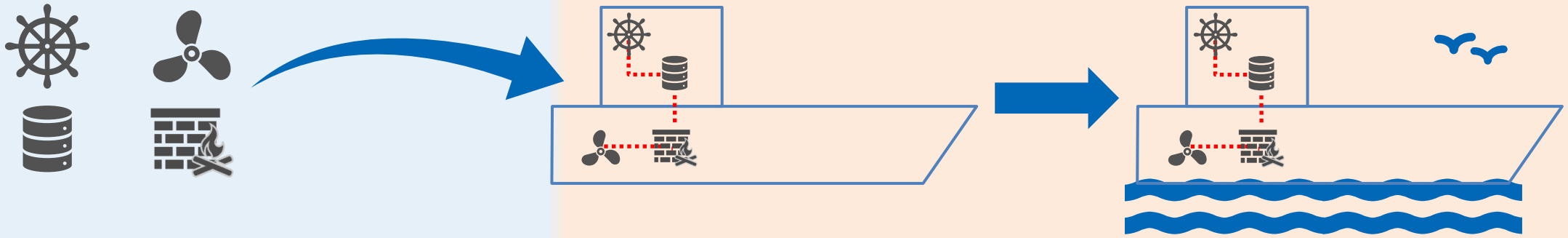
サイバーレジリエンスを考慮した機器を供給

造船所（統合者）

サイバーレジリエンスを確保した船舶を建造

船主/船舶管理会社

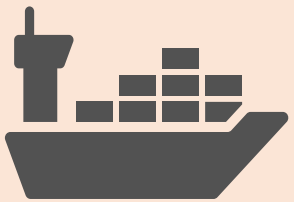
就航中の船舶のサイバーレジリエンスを維持



サイバーレジリエンスを備えた船舶を実現するための要件

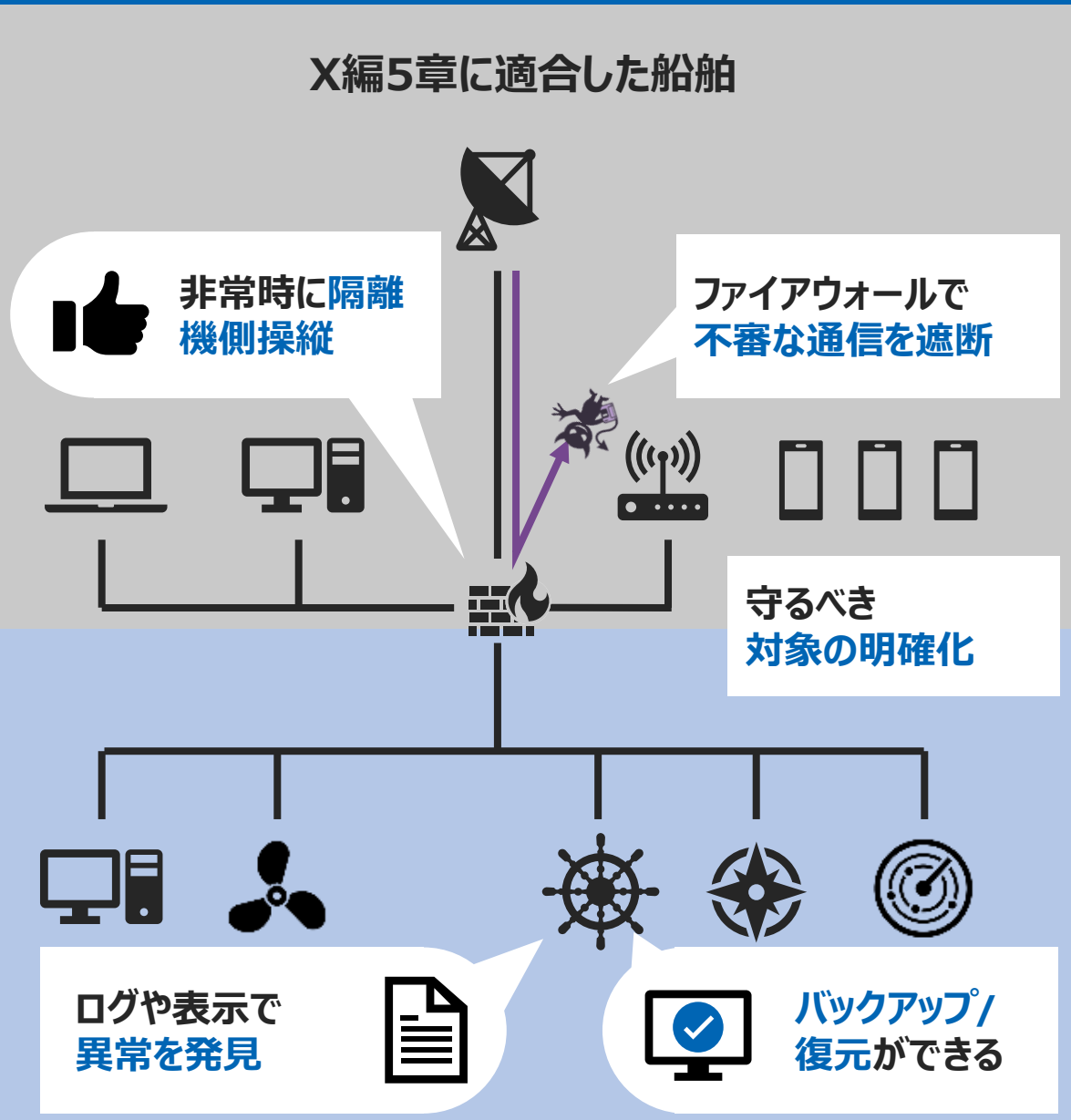
X編5章
(IACS UR E26)

「船舶のサイバーレジリエンス」



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

1. IACS UR E26の概要



識別
- 守るべきシステムを見える化し管理する

防御
- ファイアウォールで不審な通信を遮断する
- 各機器の防御機能も併用する

検知
- 各機器のログや表示で異常を発見する

対応
- 非常時は通信を遮断する
- 機側操縦に移行する

復旧
- バックアップデータで機器を復旧する

2024年7月1日以降に建造契約される下記船舶が適用対象

- 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2024年6月30日以前の建造契約の船には非強制

適用対象①：適用対象のOTシステム

適用船上で、下記機能及びシステムの運用に用いられるコンピュータシステムが適用対象

- **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、低位置、航海灯等）

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

  （例えば、緊急停止システム、荷役安全システム、圧力容器安全システム、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**

適用対象①：適用対象のOTシステム

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	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 20kW 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）
自動衝突予防援助装置（ARPA）	船首方位制御方式自動操舵装置（HCS）
音響測深機	追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

具体例についてはガイドラインをご参考ください

適用対象②③：①のシステムに付随するシステム・ネットワーク機器も対象

①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　航海

②適用対象のOTシステムと直接通信するシステム

適用対象のOTシステムと**同じセキュリティゾーンにあるシステム**

VDR・ECDIS
データサーバ

③適用対象のOT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

ここまでの①②③のシステム・機器は基本的にUR E27の承認が必要

対象外Case1：①のシステムでも、除外基準を満たすと適用対象外にできる

満たす必要のある基準

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

考慮すべき基準

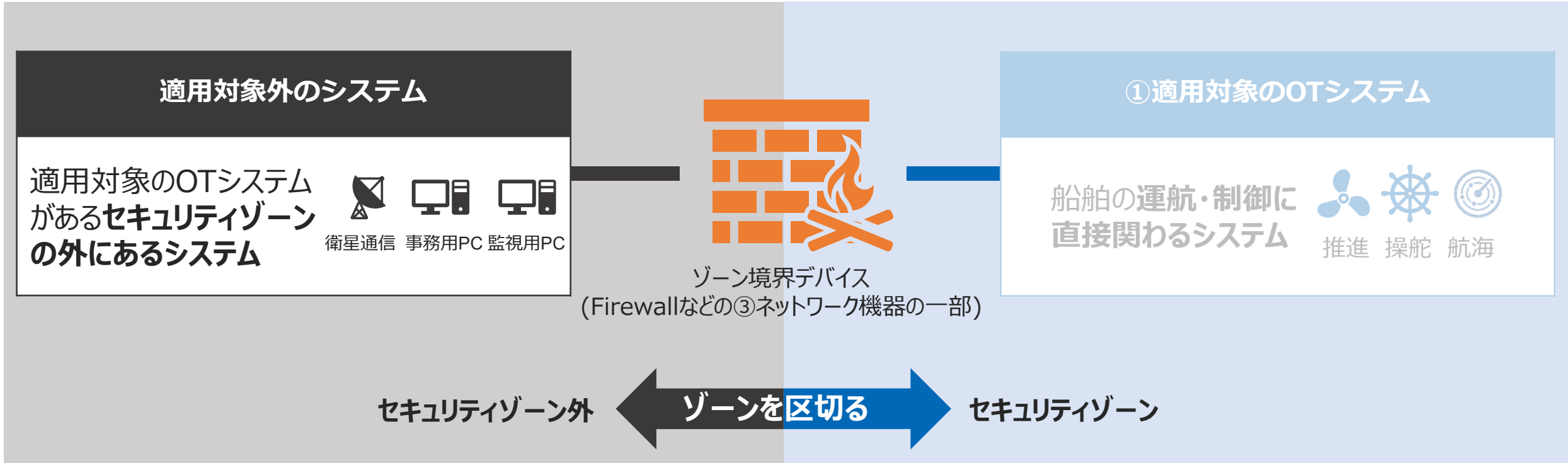
(1) 分類IIIに該当しない
(2) 脆弱性、脅威、インシデントの影響へのリスク評価が適切
(3) 攻撃対象領域が最小化されている

（完全に満たさなくても弊会が適当と認める場合受け入れ）

💡提出資料「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」にて、
上記を満たすことを**造船所が示し、弊会に承認されている必要がある**

対象外Case2：①のシステムと直接通信しないシステムは適用対象外

そもそも通信経路を設けないか、ゾーン境界デバイスで通信の制御・管理によりゾーンを区切る



対象外Case3：コンピュータを使わないシステムは適用対象外

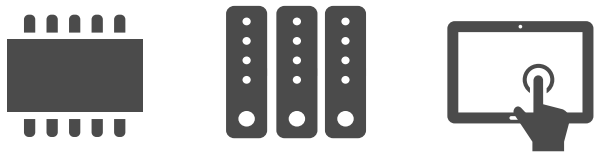
コンピュータシステムとは？

情報の収集，処理，保守，使用，共有，発信，処分等，1つ以上の定められた目的を達成するために組織化されたプログラム可能な電子デバイス又は相互運用できる複数のプログラム可能な電子デバイス

該当

適用対象

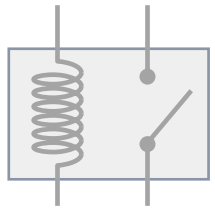
マイコン、PLC、組込み用PCなどを使用するシステムも含む



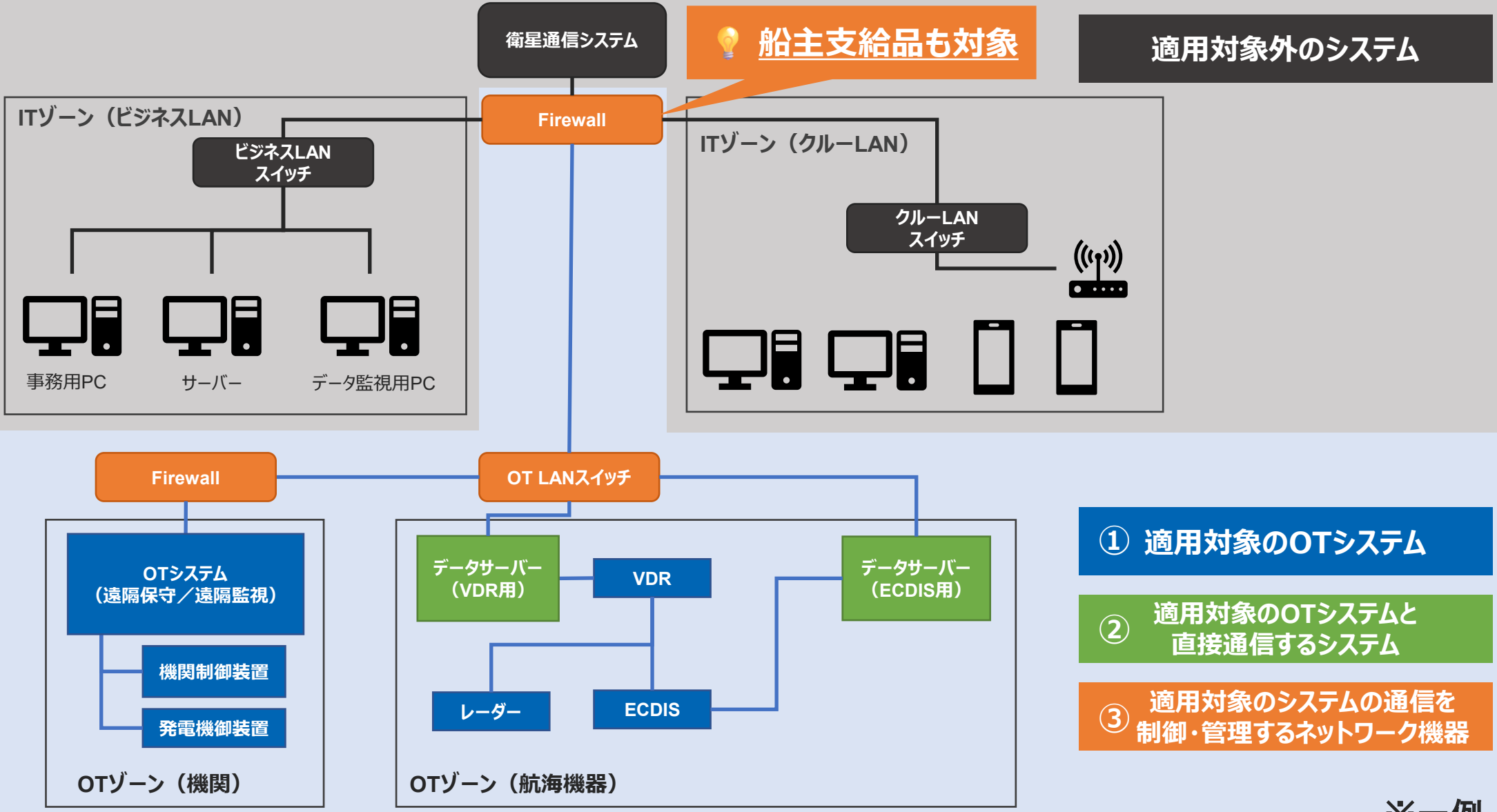
非該当

適用対象外

リレーシーケンスのシステムなど



2. 適用対象 – 適用対象のシステム・機器



① 適用対象のOTシステム

② 適用対象のOTシステムと直接通信するシステム

③ 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

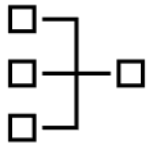
※一例

3. 適合のためのプロセス

設計段階

建造・試運転段階

①適用対象の特定



ネットワーク構成を設計し、
適用対象のコンピュータシステムを特定するための資料を作成

NKへの提出資料

「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」

②船舶の設計

供給者からの情報に基づき、
各セキュリティ要件に対する対策や設計に関する資料を作成

NKへの提出資料

「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」

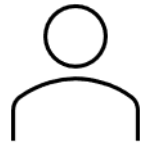
③資料のアップデート 試験要領書の作成

必要に応じて、①、②で承認された
資料をアップデート
NKの立会い検査で使用する
試験要領書を作成

NKへの提出資料

「船舶サイバーレジリエンス試験要領書」

④NK検査



「船舶サイバーレジリエンス試験要領書」に従って、**立会のもと検査を実施**

💡 **①の提出資料を事前に提出いただくことで、適用対象機器が概ね確定し、その後の提出資料の承認がスムーズになる**

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

ClassNK

船舶資産インベントリ

概要 船舶が所有するコンピュータシステム、ネットワーク機器等を一覧化した台帳

System	Detailed Machinery / Systems	Security Zone	Location	Hardware Component			Software Component		Updated Log
				Name	Model/Type	・・・	Model/Type	・・・	
Main propulsion	RCS	Machinery Zone	W/H	W/H HMI	・・・	・・・	・・・	・・・	2024.x.x
			C/R	C/R HMI	・・・	・・・	・・・	・・・	2024.x.x
Main propulsion	AMS	Machinery Zone	C/R	Main computer	・・・	・・・	・・・	・・・	2024.x.x
			W/H Accommodations	Extension panel	・・・	・・・	・・・	・・・	2024.x.x
Navigation	ECDIS	Navigation Zone	W/H	HMI	・・・	・・・	・・・	・・・	2024.x.x
			W/H	Main unit	・・・	・・・	・・・	・・・	2024.x.x

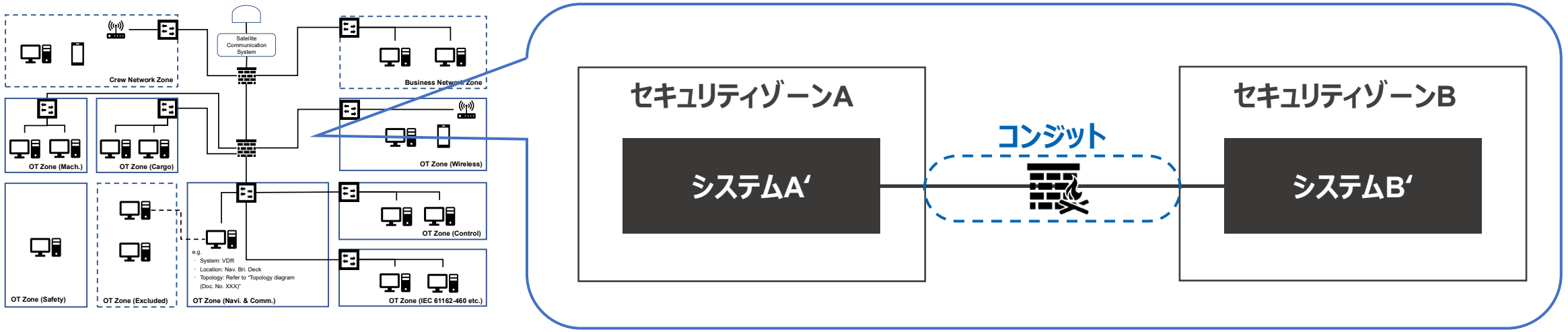
メーカが作成する
コンピュータシステム資産インベントリの情報

- 適用対象に含まれるコンピュータシステムを全て記載。**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
- 未定事項はその旨記載してNKに提出。ただし、遅くとも試運転段階での検査までに最終化し改正。

ゾーン及びコンジット図

概要

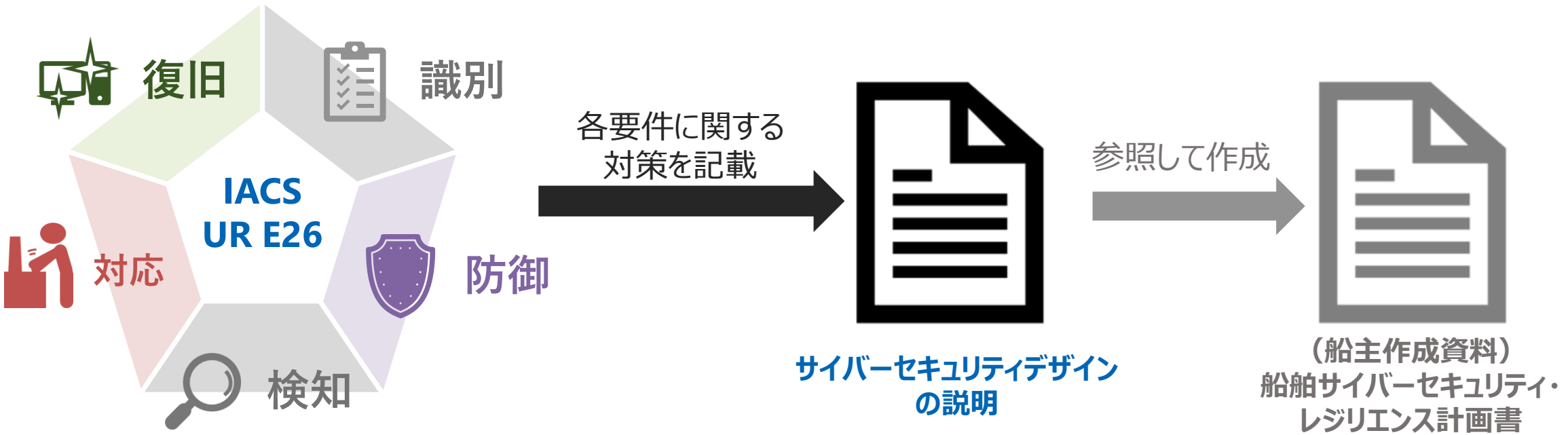
船上のネットワーク構成を視覚的に表現した図で、**セキュリティゾーン**（セキュリティレベルの異なる領域）と**コンジット**（ゾーン間の通信経路）の関係を示す



✓ 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。

サイバーセキュリティデザインの説明

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資料



✓ 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

サイバーセキュリティデザインの説明

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資料で、船主の作成する”船舶サイバーセキュリティレジリエンス計画書”が作成するために必要

例

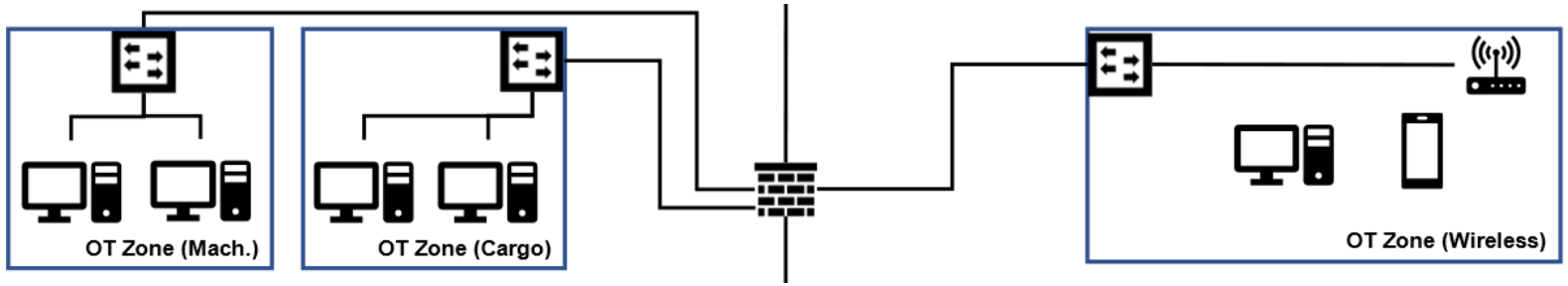
X編5.4.3(1) - 防御「セキュリティゾーン及びネットワークセグメント」

- 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の名称、用途、目的等を明示
- 同一のセキュリティゾーン内のネットワーク通信を明記

  ⇒通信の目的、通信プロトコル、データフロー
- 異なるセキュリティゾーン間のネットワーク通信を明記

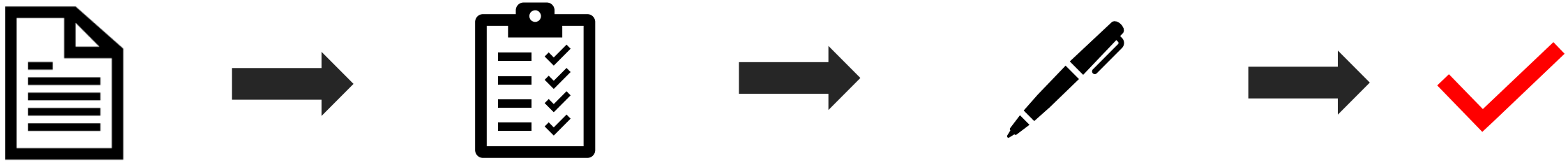
  ⇒ファイアウォール等のゾーン境界デバイスが、どのようなトラフィックを許可するか

サイバーセキュリティデザインの説明



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

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

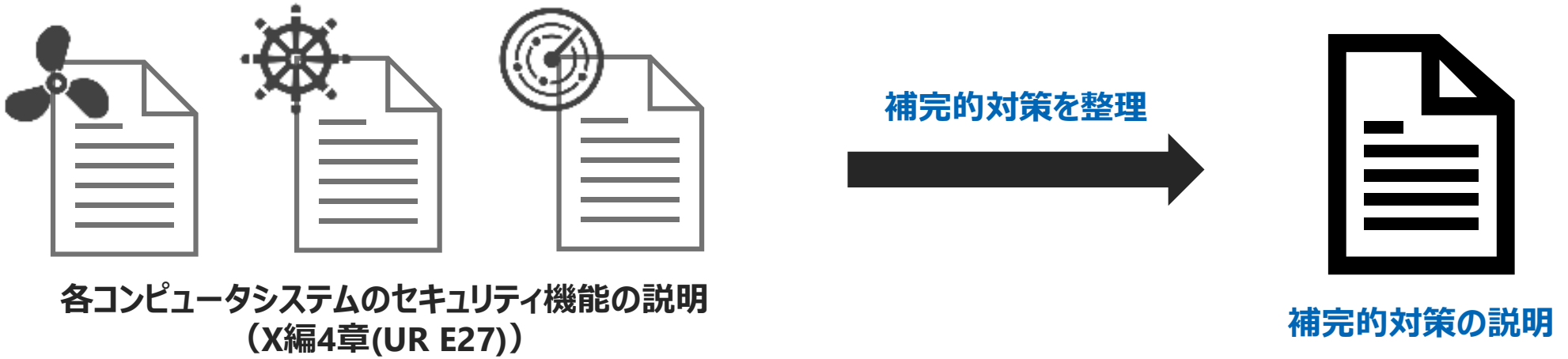


適用除外とする機器を抽出　4つの「合格基準」を満たしているか確認　3つの「追加基準」についても考慮　適用除外

- ✓ 3つの追加基準については、完全に満たさなくても弊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。

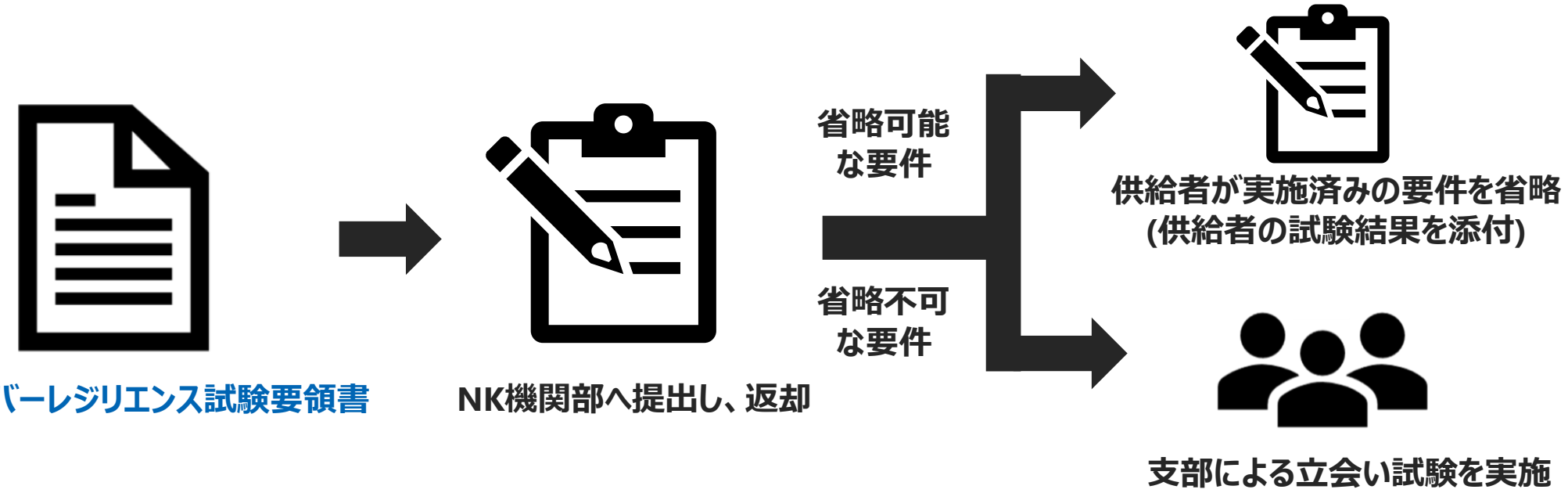
補完的対策の説明

概要 X編4章（UR E27）に規定するセキュリティ要件を、補完的対策により満たしたものをまとめた文書



- **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
- **不足しているセキュリティ機能**及びその**補完的対策**を説明
- 必要に応じた**「セキュリティ機能の説明」への参照**

検査のフロー



- いくつかの要件は、**X編4章に従うセキュリティ機能の試験**の試験結果により、**試験省略可**
- **省略が認められない要件**及びX編4章で**実施していない試験**については、**立会いが必要**
- ただし、試験要領書には**すべての試験を記載**

船舶サイバーレジリエンス試験要領書

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

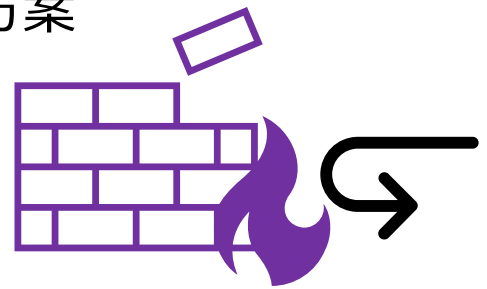
・製品ごとの試験要領を集約
・ネットワークに関する内容を追加

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**
- ✓ 船舶建造中は統合者、就航後（定期検査・システム変更時）は船主により実施される**検査に利用**

船舶サイバーレジリエンス試験要領書

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



例 **X編5.4.3(2) - 防御「ネットワークを防御する防護策」**

船舶サイバーレジリエンス試験要領書

以下に関する試験の手順を記載

- ゾーン境界デバイス(Firewall)を標的とするサービス拒否(DoS)攻撃の試験
- 各ネットワークセグメント内でのサービス拒否(DoS)の試験
- 解析的評価やポートスキャンによる、コンピュータの不要な機能,ポート,プロトコル,サービスが供給者によるハードニング指針に従い削除/禁止されていることの試験

ゾーン境界デバイス E26でのネットワークセグメントの境界となるデバイス

サービス拒否(DoS) 大量の情報送信により機器の正常動作を阻害する攻撃

ハードニング 不要な機能を無効化し、攻撃の余地を減らすこと

船舶サイバーレジリエンス試験要領書

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

例 **X編5.4.4(1) - 検知「ネットワーク動作の監視」**

船舶サイバーレジリエンス試験要領書

以下に関する試験の手順を記載

- ネットワーク接続の切断による警報の発報とその記録
- 高いネットワークトラフィックによる警報の発報とその記録
- 通信障害に対して安全に応答すること
- セキュリティ関連事象についての記録
- 侵入検知システム(IDS)が受動的で、動作に影響を与えないこと(あれば)

今後、特に以下の事項に注意が必要

- 適用範囲は**ネットワーク構成で決定**
- 以下の3つの資料は**早めに提出**(未決定項目は**その旨記載可**)
  - 船舶資産インベントリ
  - ゾーン及びコンジット図
  - 適用除外のためのリスク評価
- これら資料には**船主支給品も要記載**
- **船舶サイバーレジリエンス計画**に必要な情報は図面に要記載
- 各資料は完工時に**船主に引き渡し後本船に保管**
- 船舶サイバーレジリエンス試験要領書による**検査が必要**