# 船舶サイバーセキュリティ対策のこれから

2023年3月10日

株式会社MTI
船舶物流技術グループ

柴田 隼吾

# 目次

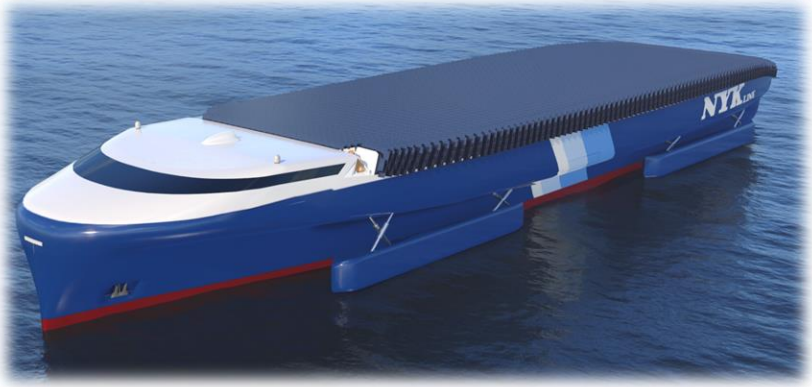

**１．はじめに**
２．船舶におけるサイバーセキュリティとは
３．業界内での議論と対応
４．今後必要とされる取り組み
５．まとめ


# 会社紹介

## 船舶・物流における安全や省エネ技術の研究開発

- 会社名：**株式会社MTI** (Monohakobi Technology Institute)
- 代表取締役：石塚 一夫
- 設立：2004年(平成16年) 4月1日
- 従業員数：64名 (2022年4月1日現在)
- 資本金：9,900万円
- 株主：日本郵船株式会社
- 本社：〒100-0005 東京都千代田区丸の内2－3－2　郵船ビル
- URL：http://www.monohakobi.com

Monohakobi Technology Institute




<u>シンガポール支店</u>

- 1 Harbour front Place #14-01,
  Harbourfront Tower One
  Singapore 098633

Monohakobi Technology Institute

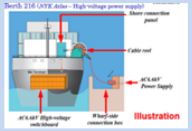
NYK GROUP

# MTIの研究開発分野

## Smarter ship and operation in NYK/MTI

Now → Future: OIL → LNG → HYDROGEN

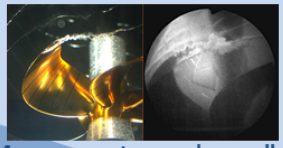
### Ship (Hardware)


Alternative Marine Power

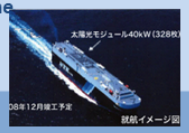

Super Eco Ship2030

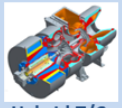

Wind Resistance Reduced
*MT-COWL*


30% Energy Saving PCTC


Measurement around propeller


Wind Power Generator
*Andromeda Leader*


Solar Panel
*Auriga Leader*

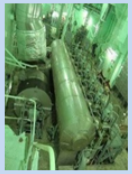

Hybrid T/C
*Shin Koho*

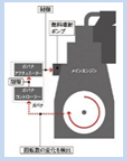

LNG-Fueled Tugboat
*Sakigake*


Innovative
Air Lubrication System
*SOYO*


LNG-Fueled PCTC
Delivery in 2016


Super Eco Ship 2050
carbon free concept ship


Electronic Controlled Engine


Improved
Governor Controller


*MT-FAST*


Air Lubrication System
*YAMATO, YAMATAI*

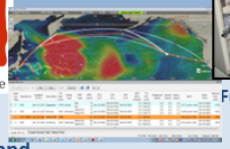

LNG Bunkering Vessel
Delivery in 2016


Hybrid Electric Power Supply
*Auriga Leader*

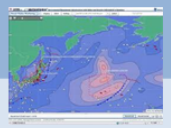

Unmanned Autonomous Ship
Trial Project (MEGURI)

### Operation (Software)


MTI Founded


NYK's own safety and
Environment standard
*NAV9000*


Fuel Consumption
Indicator
*FUELNAVI*


Prediction of
Current

Integrated Operation
Management System
NYK e-missions'


IBIS Project
Onboard Broadband
NYK SATCOM Project


LiVE
Operation Portal Site


Detection of Mach. Trouble
with monitoring data


ShipDC &
IoS-OP


24/7 Engine Plant
Monitoring Center

2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021

# 1. はじめに

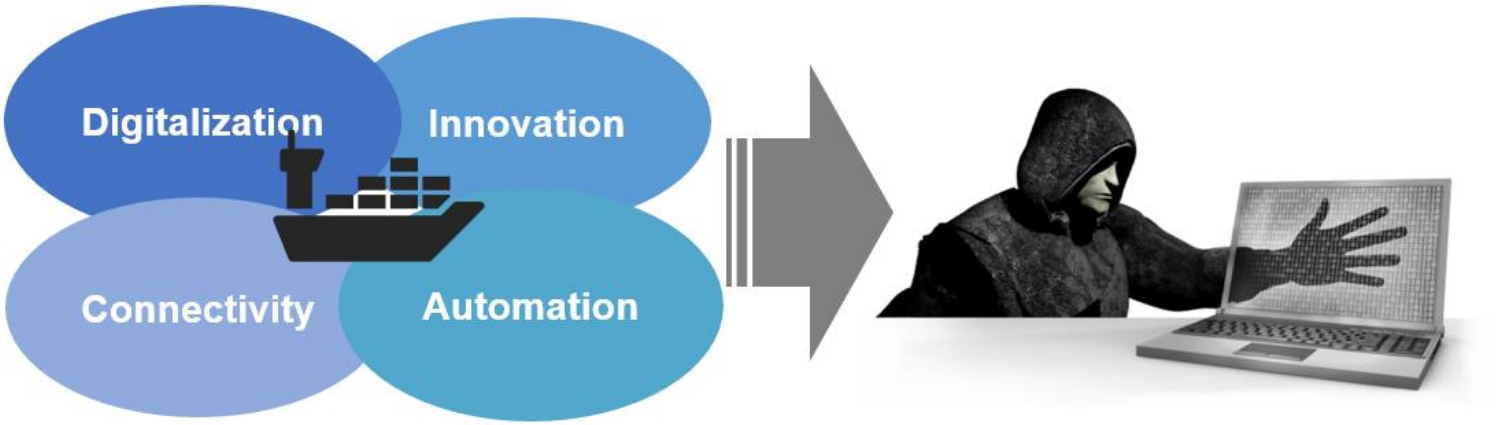
## 舶用技術の発達によりサイバーリスクも高まる

✓ICT技術の発展により、船舶の**インターネット常時接続**が普及

✓運航データの陸上モニタリングなど、**船陸間のデータ共有が急増**

⇒**機器高度化や常時接続に伴い、サイバー攻撃に晒されるリスク*が上昇**

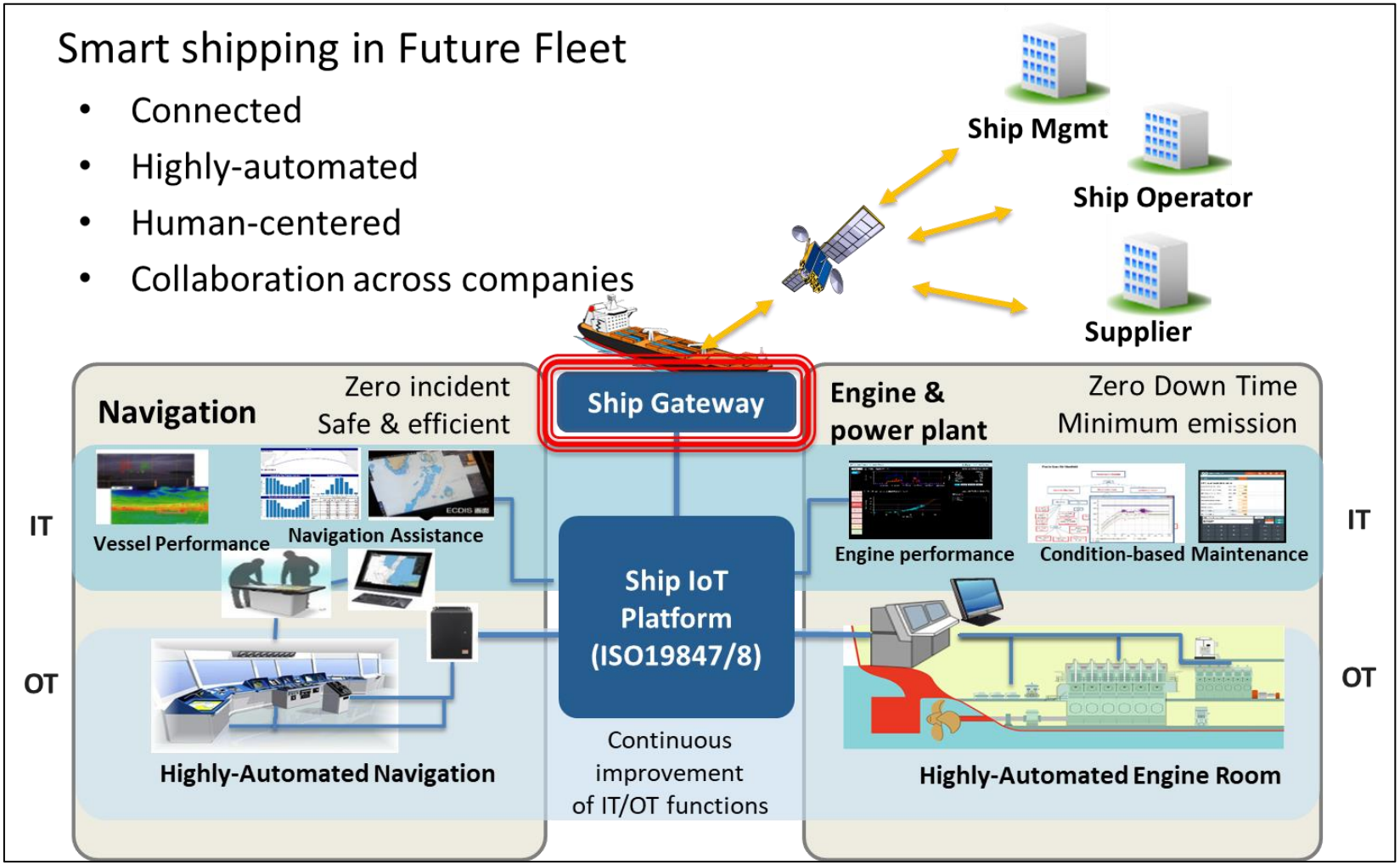
*外部からのマルウェア感染、不正アクセス等



# 1. はじめに

## 船舶IoTデータ活用の取組み事例

### 船舶高度化はますます進む

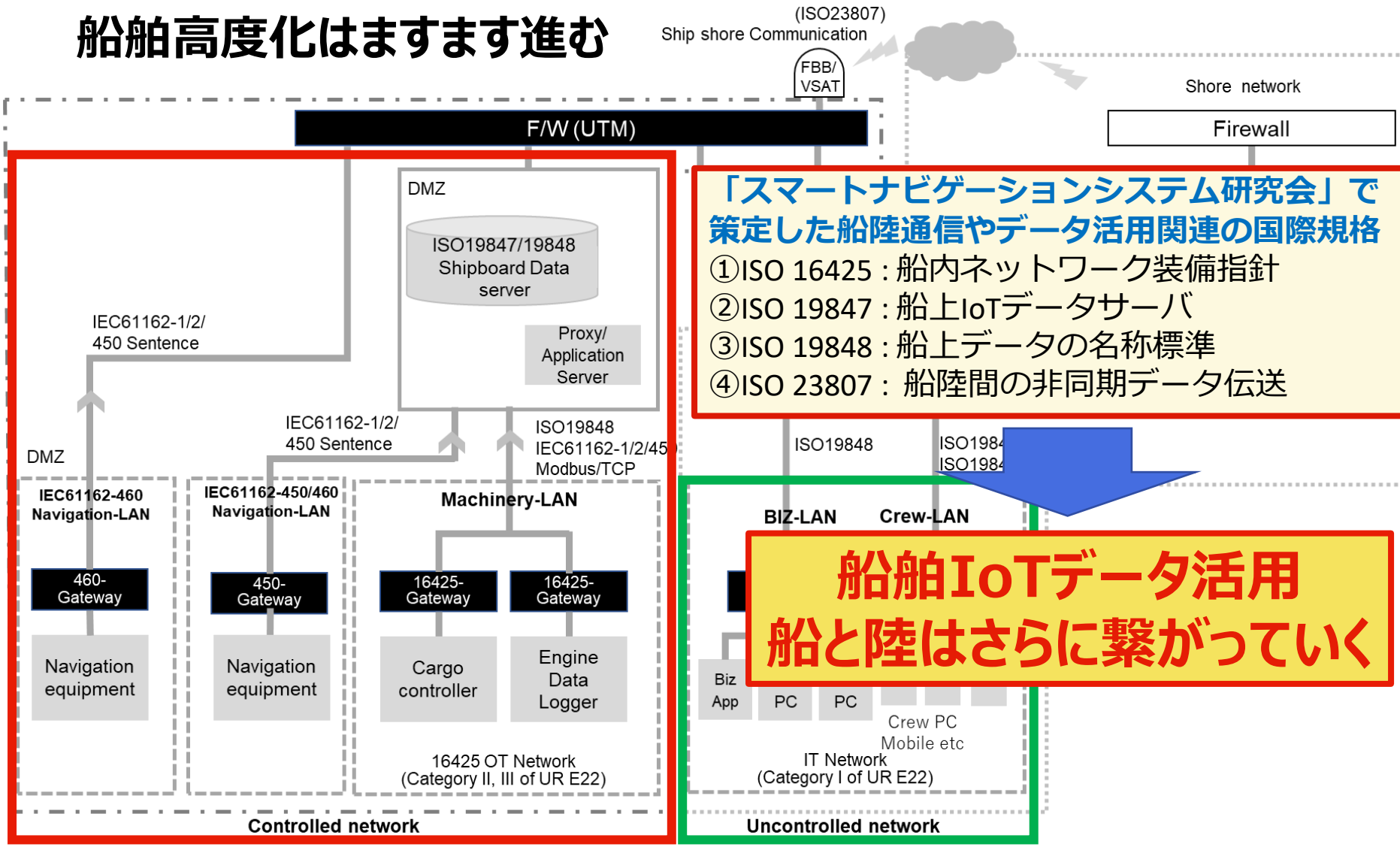



出所）ISO/TC8/WG10 Ship-shore data communication 1st panel 資料 (2019.11)

# 1. はじめに

## 船舶高度化はますます進む

# 船舶IoTデータ活用の取組み事例




**「スマートナビゲーションシステム研究会」で策定した船陸通信やデータ活用関連の国際規格**

①ISO 16425：船内ネットワーク装備指針
②ISO 19847：船上IoTデータサーバ
③ISO 19848：船上データの名称標準
④ISO 23807： 船陸間の非同期データ伝送

**船舶IoTデータ活用**
**船と陸はさらに繋がっていく**

出所） ISO/DIS 16425, 23807 規格文書より

# 目次

1．はじめに
**2．船舶におけるサイバーセキュリティとは**
3．業界内での議論と対応
4．今後必要とされる取り組み
5．まとめ

# 2-1. 海事業界でのサイバーインシデント事例

## 海事業界を狙ったサイバー攻撃がIT・OT共に急増中

### ■IT機器（主な標的：現在は陸上のシステムが中心）

| 事例発生年 | 被害 | 原因 | 被害事例 |
|---|---|---|---|
| 2017 | システム長期停止 | ランサムウェア攻撃 | Maersk |
| 2018 | システム停止 | ランサムウェア攻撃 | COSCO |
| 2020 | データセンター被害 | マルウェア感染 | MSC |
| 2020 | 一部システム被害 | ランサムウェア攻撃 | CMA-CGM |

Maersk単体
被害総額
**約330億円**

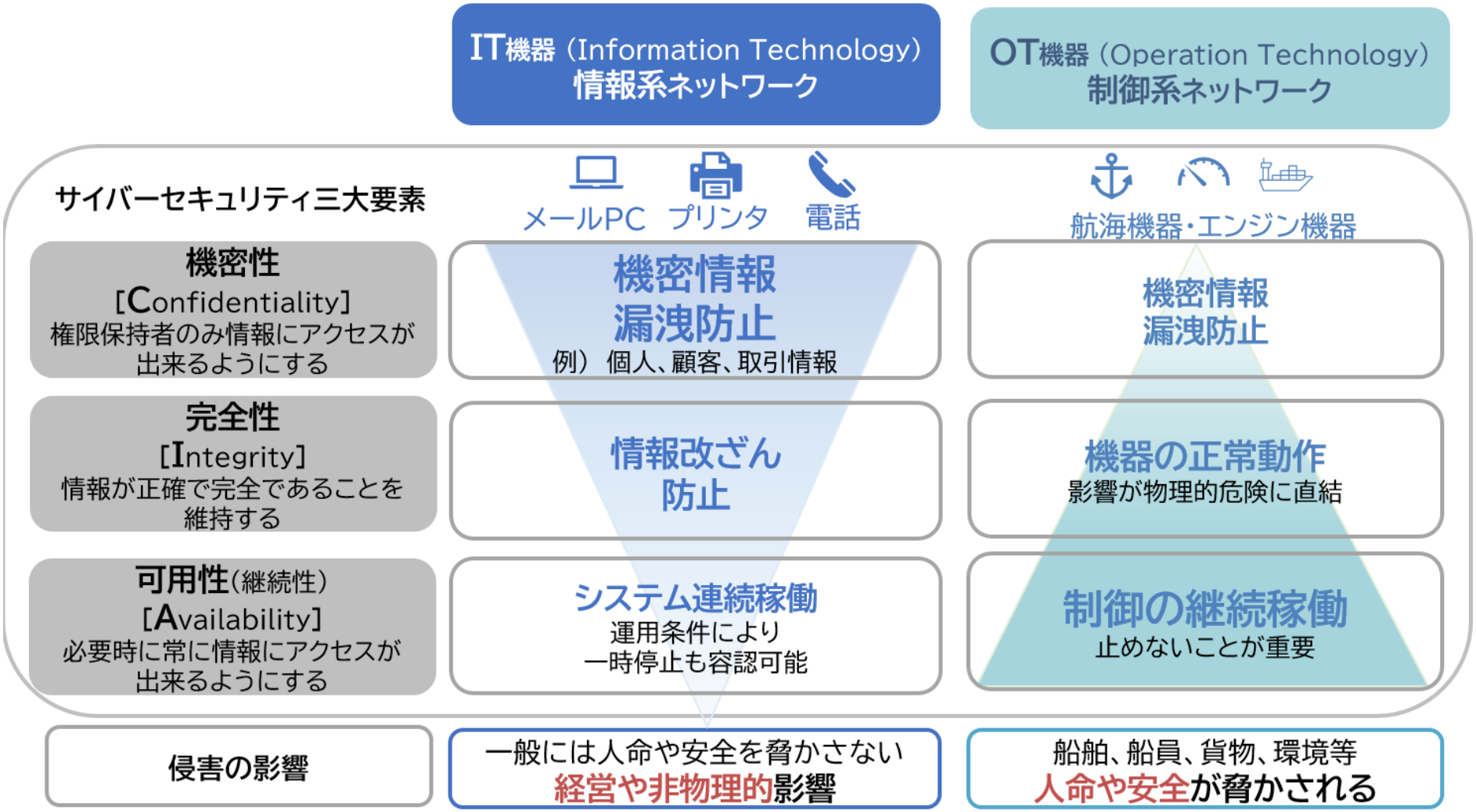
### ■OT機器（主な標的：すでに船舶も対象に）

| 事例発生年 | 被害 | 原因 | 被害事例 |
|---|---|---|---|
| 2017年頃から急増 | 船舶位置異常 | GNSS成りすまし・妨害<br><br>**G**lobal **N**avigation **S**atellite **S**ystems<br>全地球航法衛星システム。<br>GPS(米国)、準天頂衛星(日本)、<br>GLONASS(ロシア)、Galileo(EU)等の総称 | バルト海<br>黒海<br>地中海東部中央部<br>スエズ運河<br>紅海　付近等 |

出典) Above US ONLY STARS, The Center for Advanced Defense Studies 米国高等国防研究センター（C4ADS）, 2019年3月発行
出典) NORMA CYBER Annual Threat Assessment 2023

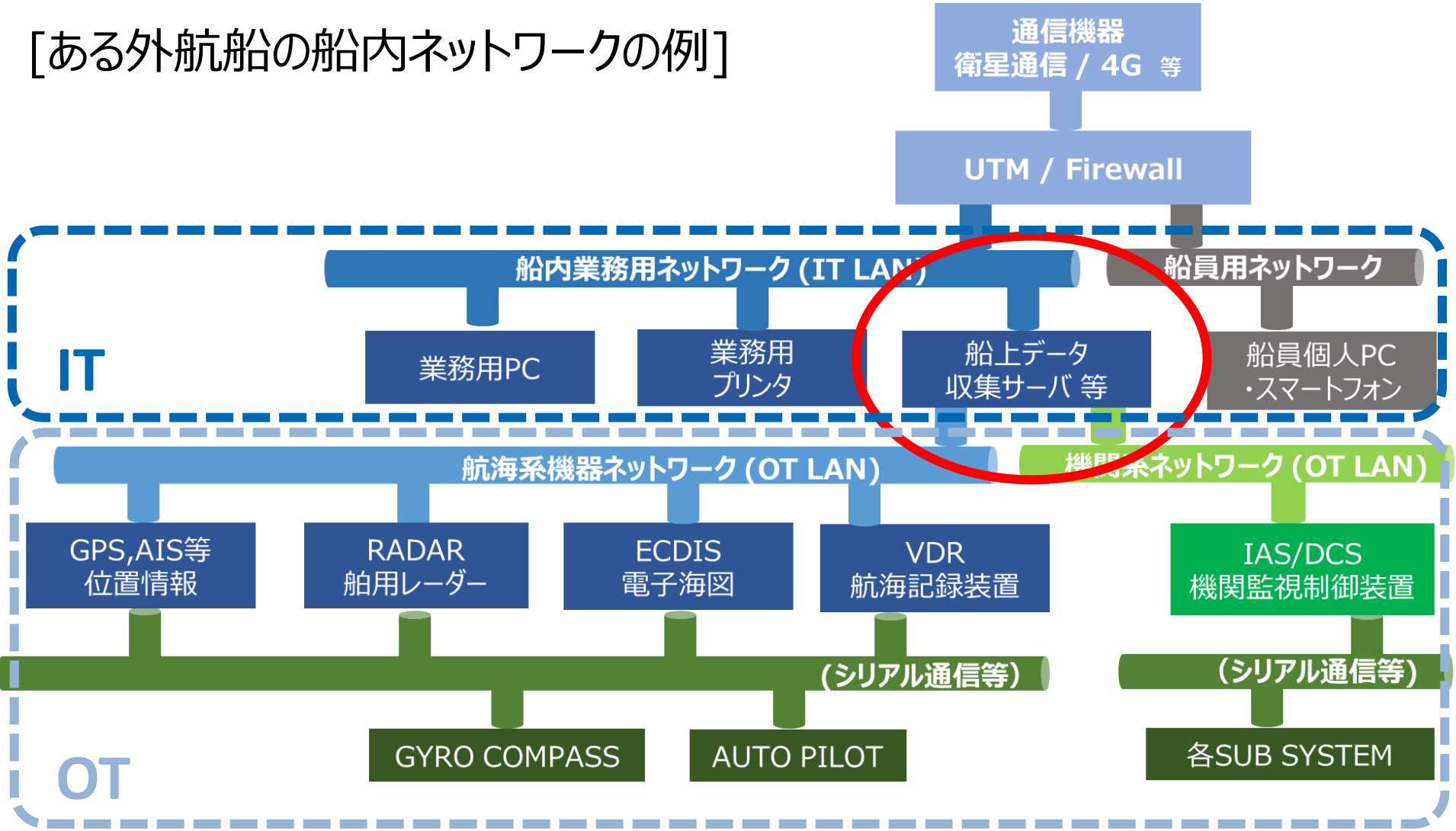
# 2-2. IT機器とOT機器

## IT機器とOT機器は セキュリティの重要要素が異なる



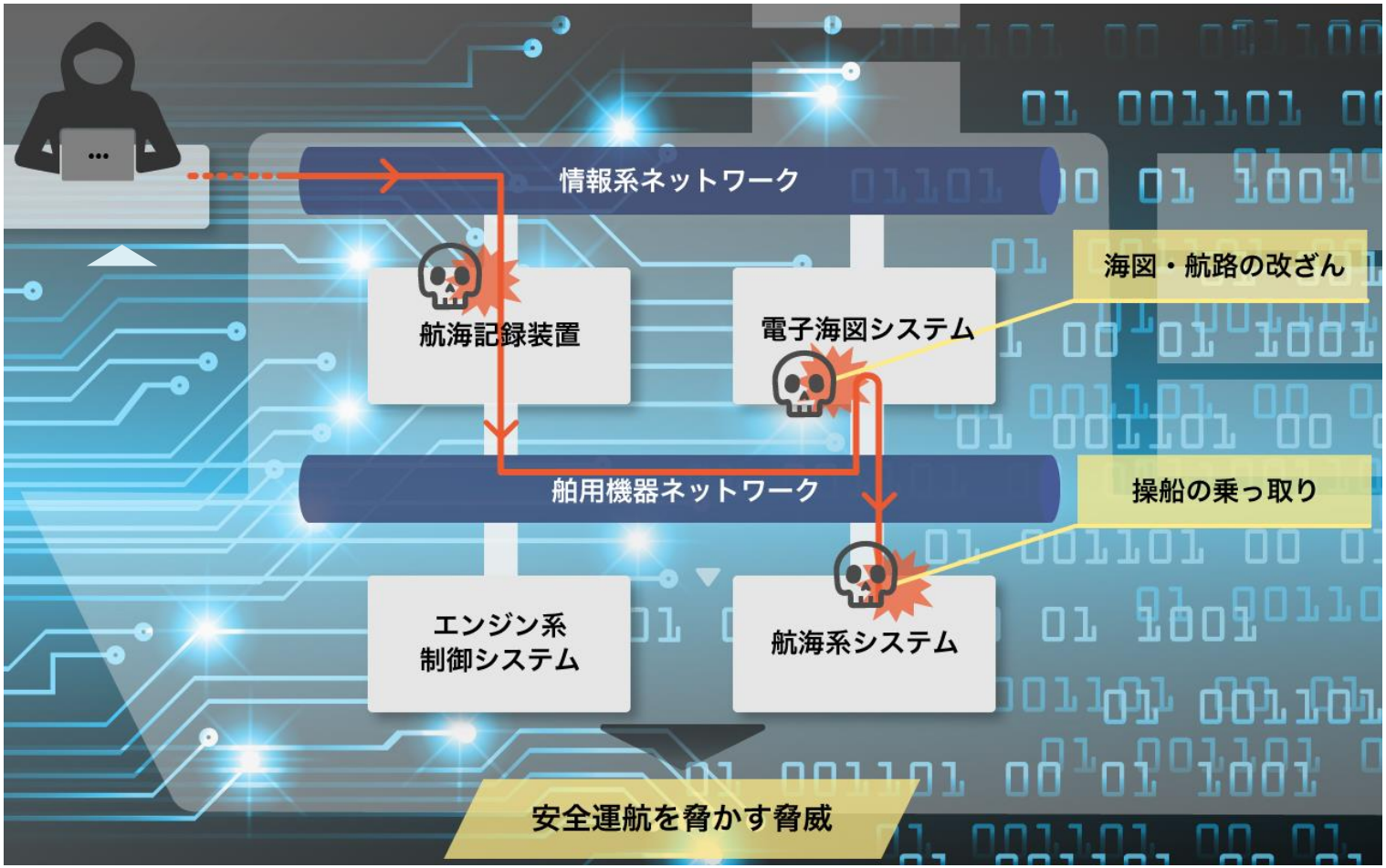
# 2-2. IT機器とOT機器

[ある外航船の船内ネットワークの例]



# 2-3. 船舶への攻撃イメージ

**船舶への攻撃は、陸のサイバー攻撃同様IT機器から始まる**



# 目次

1．はじめに
2．船舶におけるサイバーセキュリティとは
**3．業界内での議論と対応**
4．今後必要とされる取り組み
5．まとめ

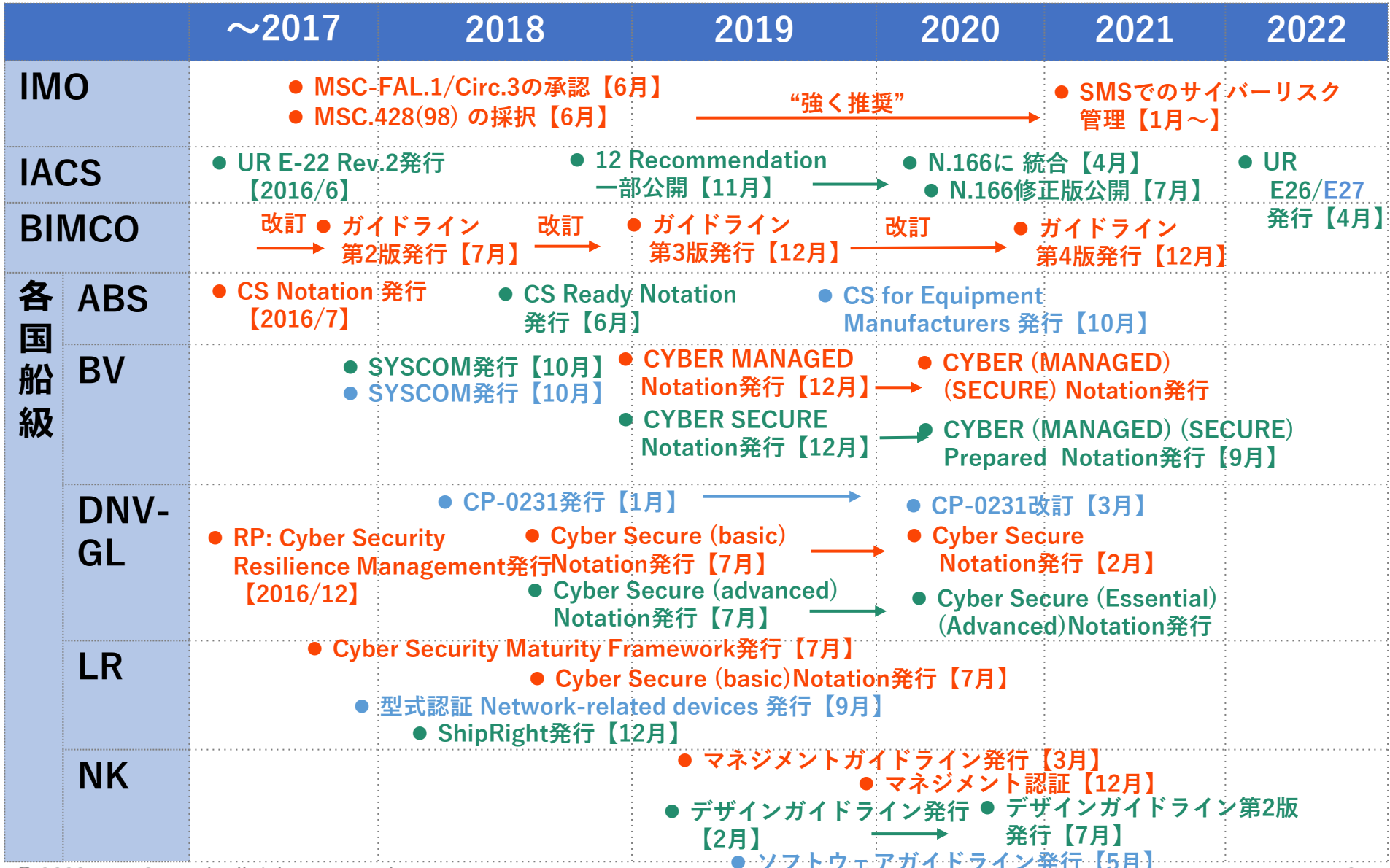
Monohakobi Technology Institute

NYK GROUP

# 3-1. IMOや各国船級の議論

凡例：
運用（船会社）に関するもの
設計・建造（造船所）に関するもの
設計・建造（メーカー）に関するもの

※当社調べ



# 3-1. IMOや各国船級の議論

## 船舶サイバーセキュリティ対策の要求レベルの強化が進んでいる

**2019 取得任意**

### 各船級協会

「**ガイドライン**」や「**ノーテーション(船級符号)・認証**」発行

**2021 強く推奨**

### IMO MSC97

SOLASの国際安全(ISM)コードにおける**安全管理システム(SMS)の中で**
船主及び運航者が**サイバーリスク管理対策を徹底**する

*SMS: Safety Management System
*ISM: International Safety Management

**2024 1月～ 強制要件**

### IACS(国際船級連合)

**サイバー耐性の強い船舶を建造・運航**するための**統一規則(UR)**発行(2022.04)

- **UR E26**：Cyber resilience of ships
- **UR E27**：Cyber resilience of on-board systems and equipment

* UR: Unified Requirements

対象｜**2024/1/1以降に建造契約する船舶の、**

a) 船内の**OT機器**（航海設備や無線通信機器を含む）
b) 当該OT機器とIPベースの通信可能な他の機器とのインタフェース

# 3-2. 船舶運航におけるサイバーリスク管理


**船舶 安全運航** — 安全で環境にやさしい運航

**安全管理システム(SMS)** — SOLAS条約 国際安全管理(ISM)コードに則った安全管理システム(SMS)

**サイバーリスク管理** — サイバーリスク管理はSMSに含めて実施することが推奨される

**サイバーリスク管理アプローチ：**

**NIST**(*1) Cybersecurity Framework
**“5つの対応カテゴリ”** に整理し改善することが多く推奨されている。

*1 NIST＝アメリカ国立標準技術研究所

①特定 (Identify)
②防御 (Protect)
③検知 (Detect)
④対応 (Respond)
⑤復旧 (Recover)

# 3-3. IACS UR E26･E27概要


## UR E26
## 船舶のサイバーレジリエンス

**要件**

**船舶全体。主に造船所／システムインテグレータ／船主向け**

**目的**

船舶の**設計から運航まで**の全工程で、**船舶のネットワークにITとOT両機器が安全に統合される**ことを目指し、**特定-防御-検知-対応-復旧**の側面からセキュリティ要件を定義。

**構成**

1. 導入
2. 用語定義
3. ゴール及び要件の構成
4. **要件 (①特定-②防御-③検知-④対応-⑤復旧)**
5. 機能評価とテストプラン
6. 本要件適用対象から除外する際に用いるリスク評価

Annex.　行動および提出書類の要約

IACS Rec 166
BIMCOガイドライン
NIST SP 800-53
IEC 62443
等を参考に規定されている

# 3-3. IACS UR E26･E27概要


## UR E27
## 船上のシステム及び機器のサイバーレジリエンス

**要件**

**個々の船上機器。主に機器ベンダ向け。**

**目的**

**機器ベンダ**により**システムの整合性を担保**するための要件を定義。
主に制御システム向け規格のIEC62443-3-3や IEC62443-4-1を引用

**構成**

1. 一般
2. セキュリティの考え方
3. 承認用に船級協会宛てに提出が必要な図書
4. **システムに関する要件**
   - **要求されるセキュリティ要件**
   - **追加のセキュリティ要件**
5. **製品の設計・開発に関する要件**

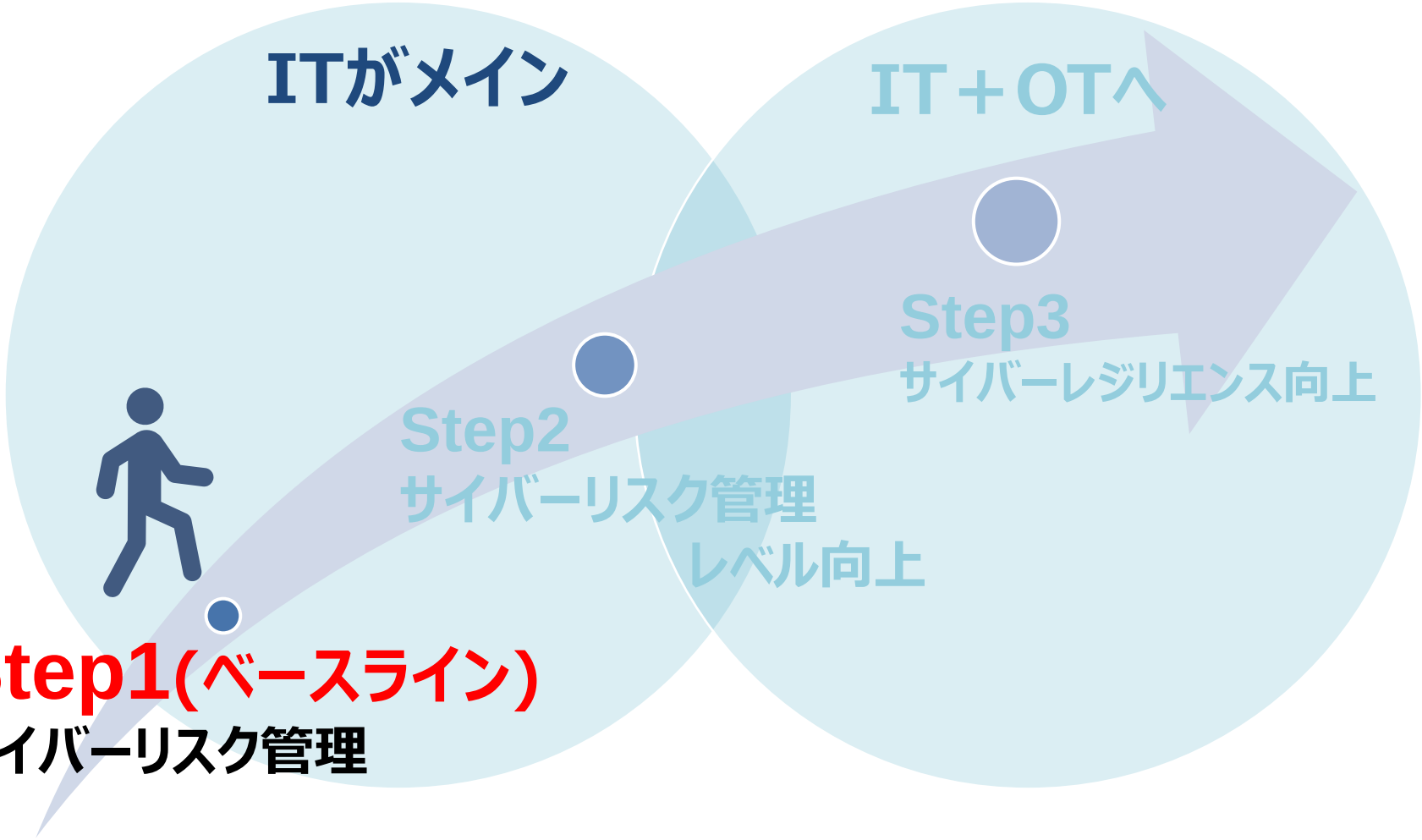
Annex. 関連するUR・参考文献

# 目次

１．はじめに
２．船舶におけるサイバーセキュリティとは
３．業界内での議論と対応
**４．今後必要とされる取り組み**
５．まとめ

# 4-1. 安全対策とサイバーリスク管理

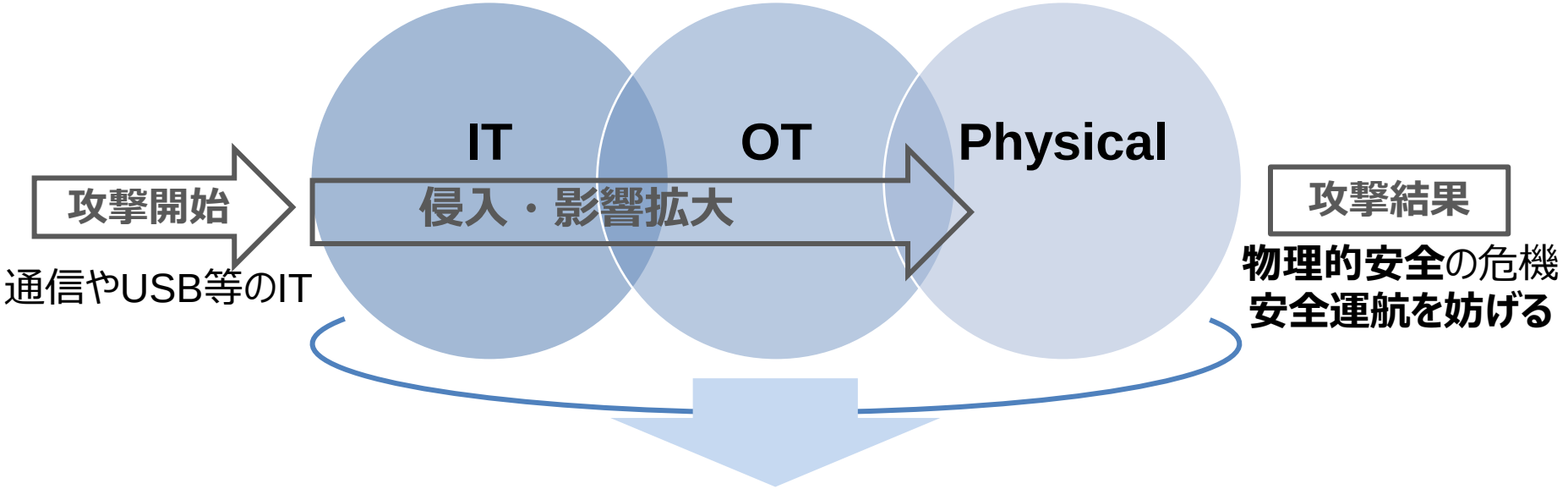
## Step1 安全管理システム(SMS)におけるサイバーリスク管理



# 4-1. 安全対策とサイバーリスク管理

安全運航を支える"**OT機器を守る**"

- **乗っ取りや運航不能の防止**
- **船舶運航機能の正常動作の維持**




**「サイバーセキュリティ」は、**
**「物理的な安全対策」とセットでの検討・対応が必要**
**"サイバー・フィジカル セキュリティ"**

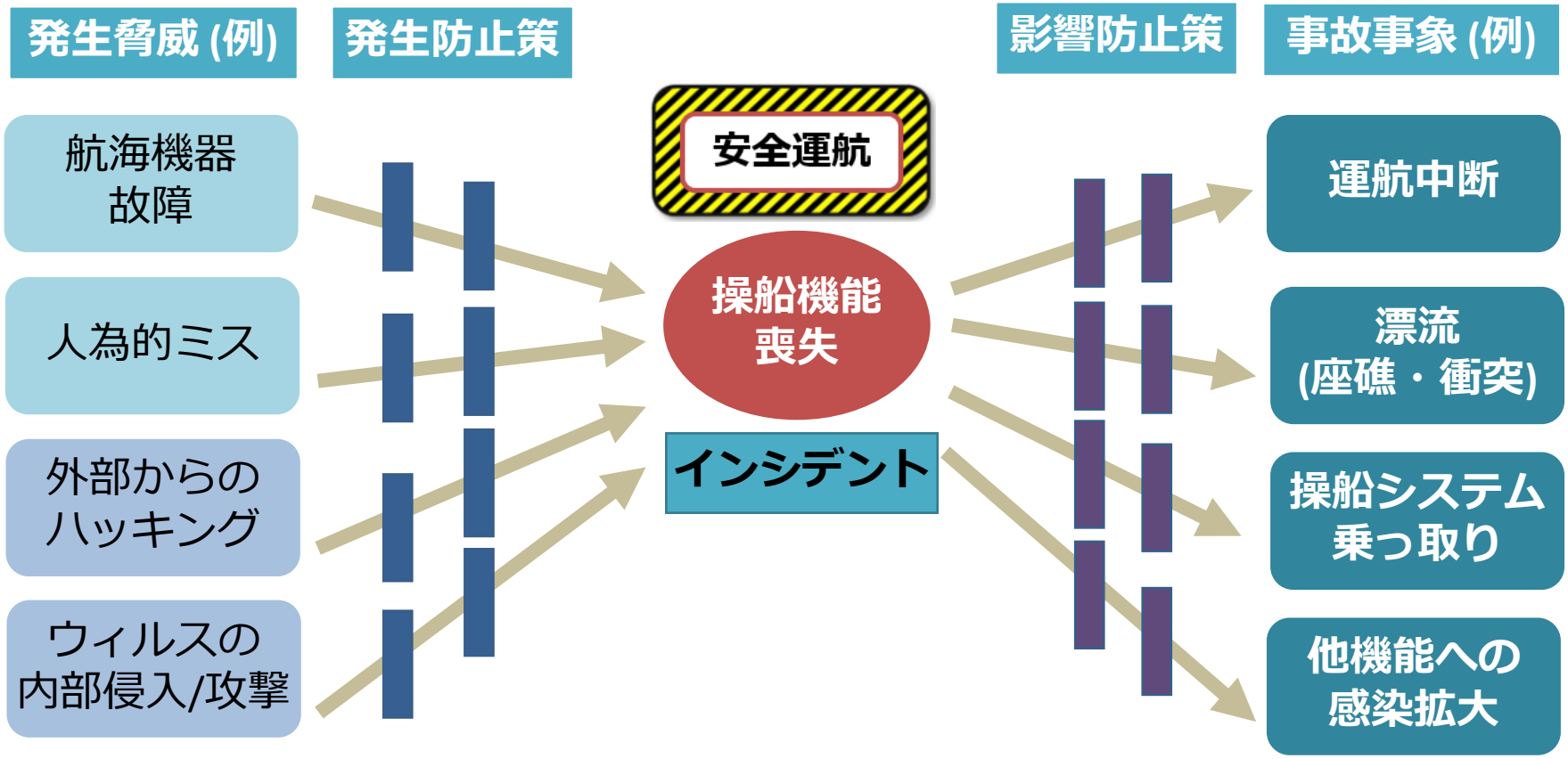
# 4-1. 安全対策とサイバーリスク管理

**サイバー攻撃の特徴**

①脅威（攻撃）の**初期症状が発見しづらい**

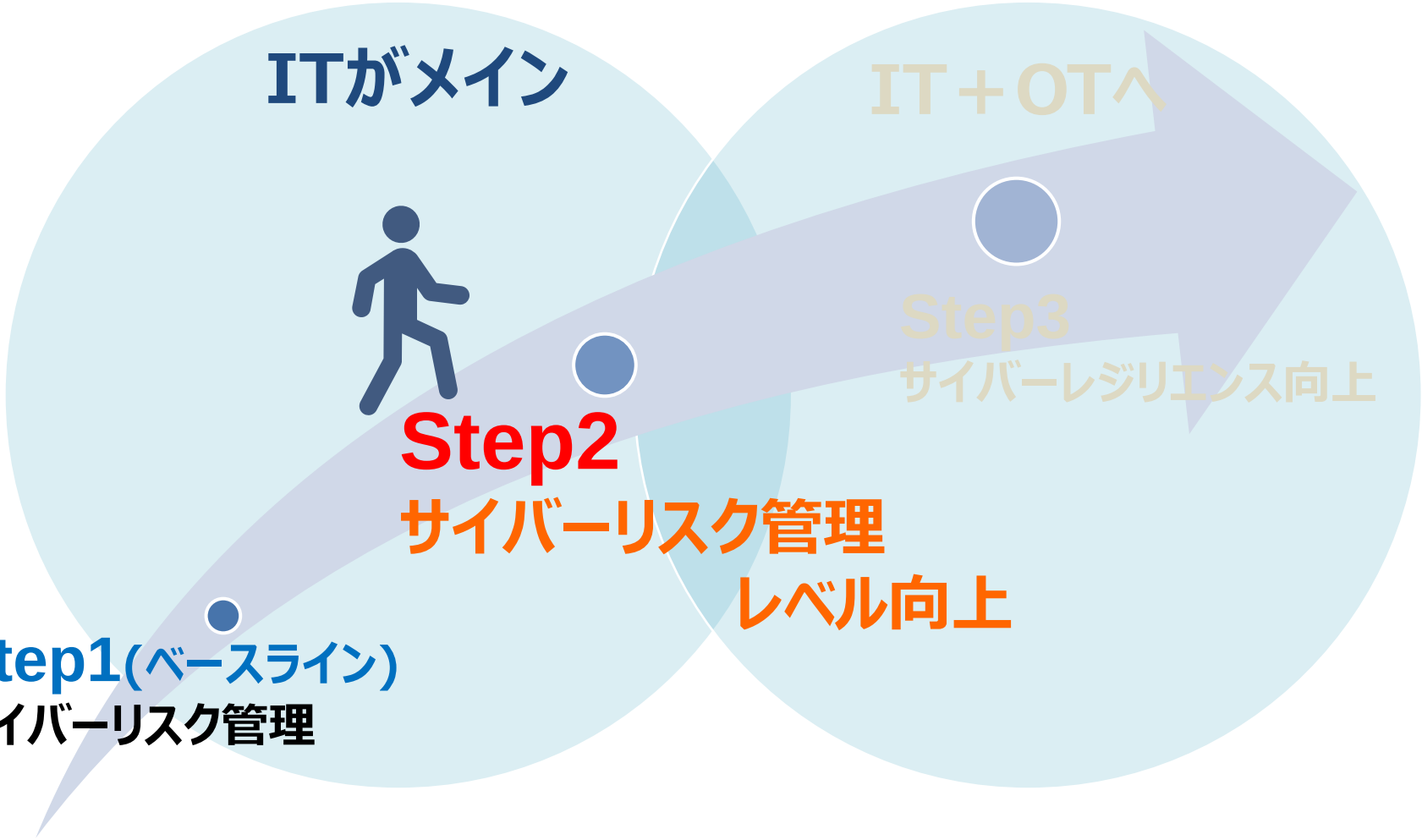
②初期対応が遅れると、影響の**拡大が速く、範囲も広い**

■Bow-Tie（蝶ネクタイ）分析手法による事例説明



# 4-2. サイバーリスク管理レベル向上

## Step2 既存のサイバーリスク管理のレベル向上



# 4-3. サイバーリスク管理レベル向上に向けた対策①

**「特定・防御」だけでなく「検知」「対応」「復旧」が重要**

特定
防御

1

船舶のサイバー**脅威**を適切に**把握**し、**防御**する。

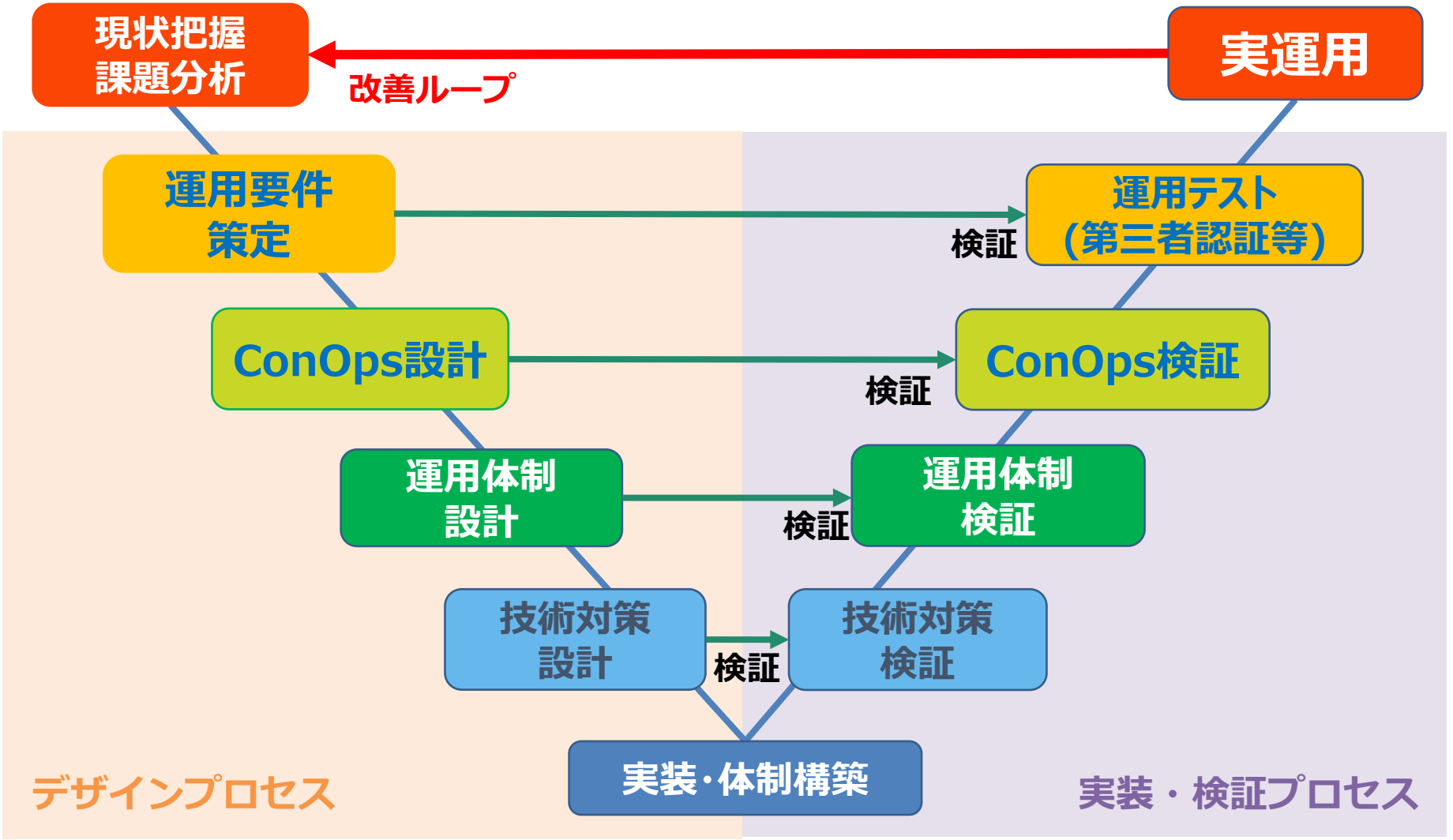
検知
対応
復旧

2

フリート全体で**統合的に集中監視**し、異常を**早期検知してインシデントを予防**する仕組み。
さらに、万が一インシデントが発生した際でも、**関係組織と連携**し、**早期対応・復旧**を**統轄**する**仕組み**と、**育成・教育体制**の構築

# 4-3. サイバーリスク管理レベル向上に向けた対策②

## 船舶サイバーリスク管理におけるV字プロセスの例

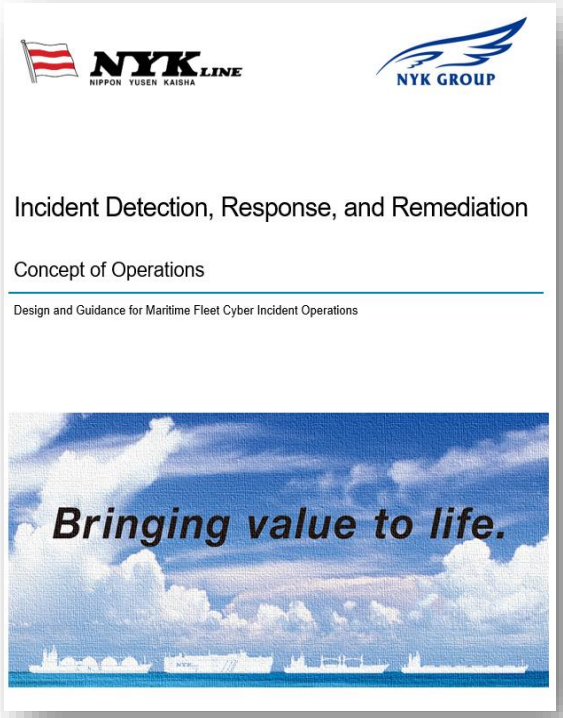


# 4-4. ConOps(運用コンセプト)の例①

## 船舶セキュリティ対応をフリート全体で進めていく

**ConOps（Concept of Operation）：運用コンセプト**

- ユーザ視点で、システム運用全体を通じた特徴や要求・機能を明確化
- ユーザー・開発者・関係者間でのシステム全体コンセプトの認識共通




・背景と目的、スコープ

・組織設計とガバナンス
　推奨組織体制図
　全体ガバナンス
　憲章テンプレート

・役割とスキル
　各組織の役割とスキルセット
　RACIチャート(責任分担表)

・技術/実装
　多層防御
　技術インテグレーション
　遠隔監視

・ロードマップ

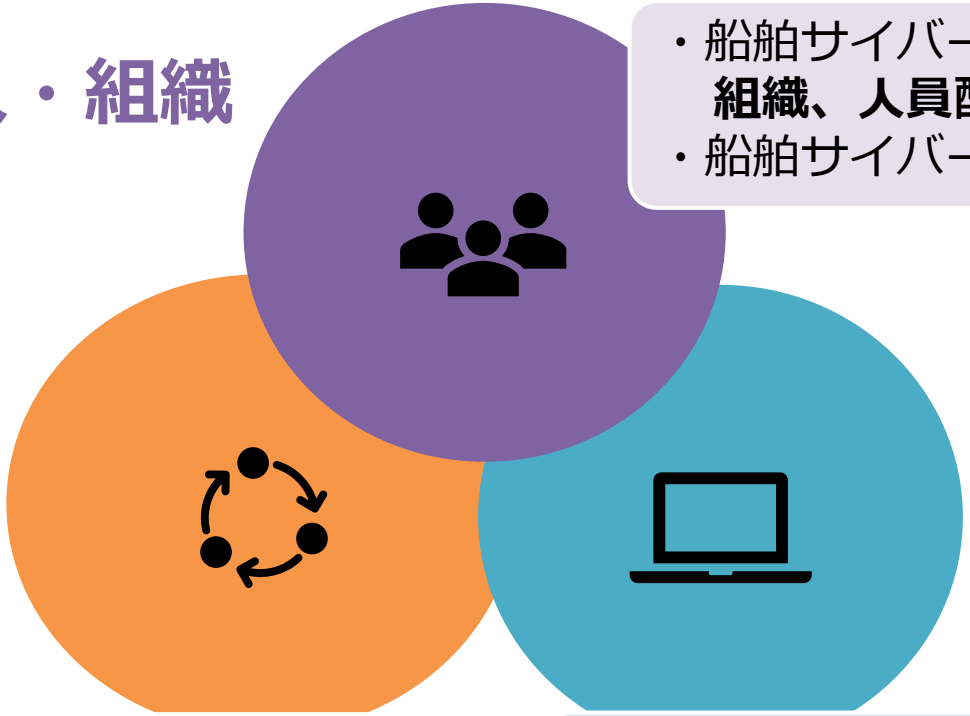
・ポリシー設計
　船舶サイバーセキュリティポリシー
　サイバーリスク管理対応ポリシー
　ポリシーの改善

・パフォーマンス管理
　パフォーマンス目標値・KPI策定

等を記載

# 4-4. ConOps(運用コンセプト)の例②

**「組織」・「プロセス」・「技術」の３側面からの強化を実施**



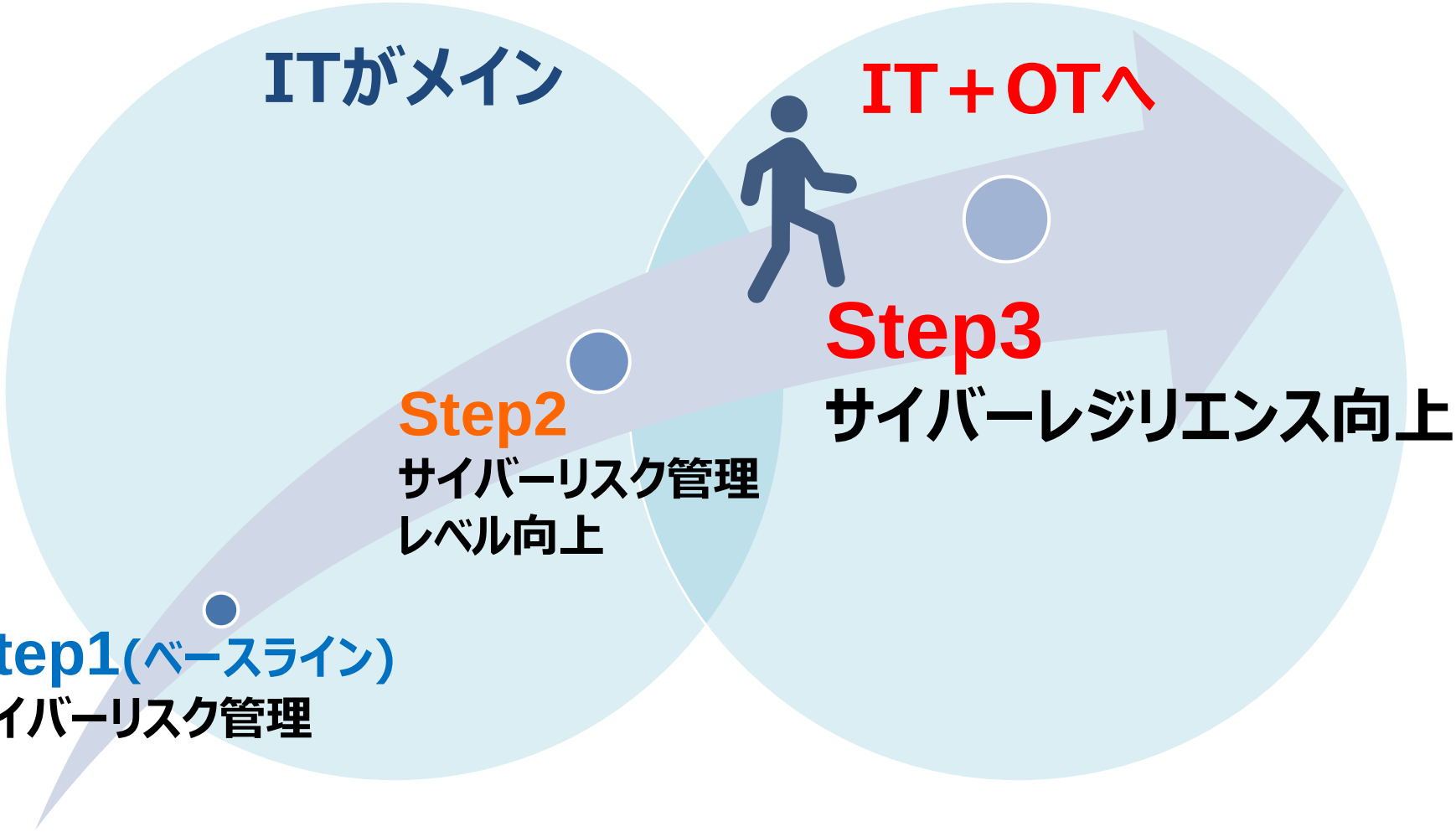

・船舶サイバーインシデント対応
**組織、人員配置の強化**
・船舶サイバー**監視組織の構築**

・インシデント対応のポリシー・プロセスの準備
・パフォーマンス目標値・KPI設定

・陸上からの**遠隔監視の仕組**の構築
・**OT**ネットワークの**異常監視**ツール

# 4-5. サイバーレジリエンスの向上

**Step3 ITの対策を進めつつ、OTへの展開も進める**



# 4-6. IACS UR E26/E27への対応①

## E26の４章「要件」の概要　（ClassNKによる仮訳版より抜粋）

4.1 **識別**(Identify) ➡ 本船にネットワークを使用して接続されるシステムを把握

- ハードウェア、ソフトウェア、ネットワーク関するインベントリを作成し、船舶の一生にわたって更新すること。

4.2 **防御**(Protect) ➡ Firewall、ルーターによるネットワークの分離

- セキュリティゾーンを超える通信は、明示的に許可されたものに限定すること。
- ファイアウォール等で防御し、過度のデータフローも防ぎ、不要な機能は制限すること。
- ウィルス対策ソフト等で防御すること。（手順や物理的保護、製造者の推奨によっても可。）
- アクセス制御として、鍵を掛け、部外者によるアクセスは監視下に限り、取外し可能なメディアの使用も管理し、アクセス権も管理し、最小権限の原則を適用する等を行うこと。
- 無線通信は、許可された人／プロセス／デバイスに限定し、暗号化等も活用すること。
- リモートアクセスは明示的な許可を要し、ログを残す等して、保守時もロールバックや多要素認証等を求め、アクセス失敗後一定時間は再試行不可、多数失敗でブロック等を行うこと。
- モバイルデバイスの接続は、船舶の運航や保守に必要ないものはブロックすること。

# 4-6. IACS UR E26/E27への対応②

4.3 **検知**(Detect) ➡ 不正アクセスの監視

- ネットワークを監視し、過大なトラフィックや不正な接続等の異常時に警報を発すること。

4.4 **対応**(Respond) ➡ インシデント準備と対応

- インシデント対応計画書を、設計の情報も集めて、初回年次検査までに作り、船の一生にわたり更新し、紙で保持すること。
- バックアップの機側制御は、主制御システムから独立し、監視も制御も自己完結していること。
- ネットワークの分離は、手動又は自動で物理的に実行でき、データ依存性も明示しておくこと。
- 機能不全時にミニマムリスクコンディション（状況に応じた低リスクの停止状態等）に至ること。（機能不全時の状況を把握すること）

4.5 **復旧**(Recover) ➡ インシデント発生後の復旧方法を明確にする

- 復旧計画書を、設計の情報（復旧やバックアップの手順、ネットワークの構成図等）も集めて、初回年次検査時までに作り、船の一生にわたり更新し、船上及び陸上に紙で保持すること。
- バックアップ計画書を作成し、バックアップ及びリストアが、適時に完全に安全に行えること。
- 制御されたシャットダウン、リセット、ロールバック、再起動が手順(書)に従って行えること。

# 4-7. 船舶OTにおける「検知」（監視・モニタリング）

## モニタリングはIACS UR E26で要求事項となる

**IACS UR E26引用　仮訳**

### 4.3.1　ネットワーク動作の監視

**4.3.1.1 要件**

本URの適用範囲内にあるネットワークは、
- ✓ **連続的に監視**されなければならない。
- ✓ **故障又は機能低下の際には、警報が発せられ**なければならない。

**4.3.1.3 要件詳細**

本URの適用範囲内にあるネットワークを監視する手段は、以下が可能である必要がある。
- ✓ **過度のトラフィック**の監視及び検知
- ✓ **ネットワーク接続**の監視
- ✓ **デバイス管理活動**の監視及び記録
- ✓ **権限を与えられていない機器の接続**の監視又は防御

# 4-7. 船舶OTにおける「検知」（監視・モニタリング）

## OTモニタリングツールの例　（当社にて検証実施）

| | |
|---|---|
| **ツール概要** | PLC等の**OTプロトコルに対応**する**セキュリティモニタリングサービス**<br>*PLC(Programmable logic controller): 機器制御に使われるコントローラー |
| **主要機能** | 1. アセットの管理<br>2. ネットワークマップの自動生成<br>3. ポリシーの設定、イベントの検知・通知<br>4. 通信状況の可視化<br>5. モニタリング結果を統括したセキュリティレポートの作成 |
| **検証対象** | 船舶の操船系機器を模擬した環境 |
| **検証方法** | 検証環境にモニタリングツールを接続して通信されるパケットをキャプチャし、自動解析結果を検証。 |

**アセットの管理**

**通信状況の可視化**

**ポリシーの設定・イベントの検出・通知**

# 4-8. さらなるサイバーレジリエンス向上に向けて①

## 船舶ペネトレーションテスト検証プロジェクト (2019～2020年)

**海運業界の各プレイヤーが連携**し、専門家の協力を仰ぎながら、船舶における
ペネトレーションテストの**知見獲得**と、検証手段としての**各種課題の抽出**を目的に実施

| 役割 | 企業名 | 業種 |
|---|---|---|
| プロジェクト統括 | ジャパン　マリンユナイテッド　株式会社 (JMU) | 造船会社 |
| | 株式会社ＭＴＩ | 船会社 研究機関 |
| 被験機器・システム主管 | 寺崎電気産業 株式会社　（機関系） | 舶用機器メーカ |
| | 東京計器 株式会社　（航海系） | |
| | ナブテスコ 株式会社　（機関系） | |
| | 日本無線 株式会社　（航海系） | |
| | BEMAC 株式会社　（機関系） | |
| | 古野電気 株式会社　（航海系） | |
| アドバイザリー | 一般社団法人 日本海事協会 | 船級協会 |
| | 日本郵船 株式会社 | 船会社 |
| テスト運営支援 | 株式会社 ＮＴＴデータ | ＩＴ・サイバーセキュリティ専門企業 |
| テスト実行 | 株式会社 イエラエセキュリティ | |

➡ ClassNK殿 Webサイトにて本検証の成果報告書 公開中
https://www.classnk.or.jp/hp/pdf/press/report/202007j.pdf

# 4-8. さらなるサイバーレジリエンス向上に向けて②

**他産業や国内外での先行事例も参考にし、船舶サイバーレジリエンス向上を目指す**

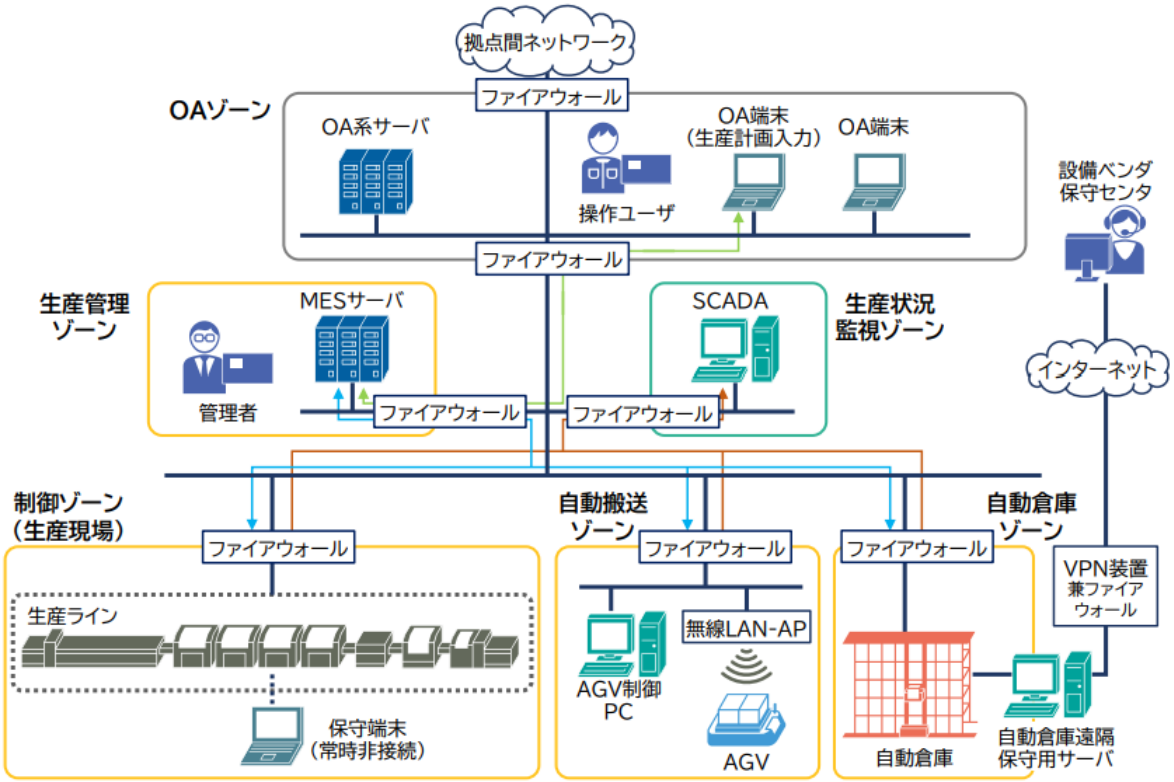




図 3-3 要件に対する各ゾーンでの対策(例)

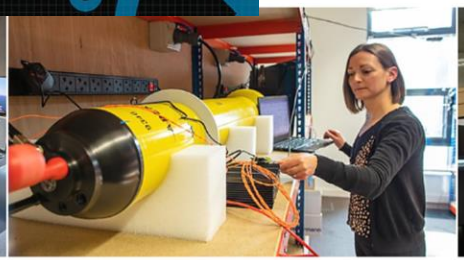
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

※まず、付録Ｅのチェックリスト実施がおすすめ

# 4-8. さらなるサイバーレジリエンス向上に向けて②

**他産業や国内外での先行事例も参考にし、船舶サイバーレジリエンス向上を目指す**

Cyber-SHIP Lab
SECURING MARITIME



## Creating ships systems' physical twins in the Lab

Cyber-SHIP Lab brings together an endlessly configurable host of connected maritime systems found on ships' bridges – equipment commonly deployed across international fleets, configured and re-configured in vessel or vessel-type-specific layouts. It can effectively become a physical twin of any ship's bridge and associated OT.

Cyber-SHIP Lab provides insights that cannot be gained in the virtual world through simulation alone.

The Lab's unique hardware-based testbed complements the University's fleet of nine ship simulators and our cyber ranges. Research outputs – including real-world attacks on non-virtual machines – are used to make researchers' and crews' simulator experiences much more realistic and useful for training as well as securing devices.

Uniquely, this means we can use the Cyber-SHIP platform to determine **physical systems'** key vulnerabilities under a range of cyber attacks. It

## Work with us

Industry and wider maritime sect
the project. Cyber-SHIP Lab is c
and maritime-related sector partners, including ship operators and companies involved in the supply of hardware and software, construction of ship's bridges and training and management of personnel. We are also working with classification societies and government cyber security agencies.

Such industry engagement is vital. It is only by working with those in the sector that we can develop solutions applicable in the real world.

**We are seeking additional partners to collaborate with us in building maritime cyber threat resilience. Whether your interest is in shaping collaborative research, meeting future training needs, or ensuring systems' resilience, please contact Cyber SHIP-Lab Project Manager Chloe Rowland to discuss how your organisation can join us in this pioneering maritime security project.**

https://www.plymouth.ac.uk/research/cyber-ship-lab

# 目次


1．はじめに
2．船舶におけるサイバーセキュリティとは
3．業界内での議論と対応
4．今後必要とされる取り組み
5．まとめ


# 5. まとめ①

## 1. 船舶におけるサイバーセキュリティ

✓ 船舶でもITとOTが繋がりつつあるが、**それぞれにあった対策**が必要

## 2. 業界内での議論と対応

✓ 船舶サイバーセキュリティ対応の要求レベルが強化されている

✓ IACSは2024年1月1日以降に建造契約がされる船舶を対象に、**UR E26**(船舶全体向け)、**UR E27**(船上の個々の機器向け)を発行

## 3. 今後必要とされる取り組み

✓ **物理的安全対策と連携した "サイバー・フィジカルセキュリティ"**

✓ 船舶IT・OTにおいて、早期に**「検知」**して**「対応」**し、**「復旧」**させるための**「技術・プロセス・組織」の構築**が今後必要とされる。

✓ 船舶ペネトレーションテスト実施には業界内での継続議論が必要

✓ 規則ミニマムの対応ではなく、他産業や国内外先行の事例も参考にして、船舶サイバーレジリエンス レベルの向上を目指すべき。

# 5. まとめ②

**ITの対策を進めつつ、対策のOTへの展開準備を進める**

ITがメイン

IT＋OTへ

**Step1(ベースライン)**

**サイバーリスク管理**

・物理的安全対策との連携
“サイバー・フィジカルセキュリティ”

**Step2**

**サイバーリスク管理**
**レベル向上**

・船舶**IT機器の「検知」「対応」**
・**フリート全体の統合監視対応**

**Step3**

**サイバーレジリエンス向上**

・IACS UR E26/E27対応
・船舶**OT機器も「検知」「対応」**
・ペネトレーションテスト検討
・**「プロセス」・「組織」**の構築

Monohakobi Technology Institute

NYK GROUP

# ご清聴ありがとうございました。

Monohakobi Technology Institute

参考資料

NYK GROUP

# 船舶のOT機器のモニタリング技術検証 –アセットの管理–

アセットの管理

## アセット結果イメージ

| アセット | タイプ | リスク値 | 重要度 | IPアドレス | カテゴリ | ベンダ |
|---|---|---|---|---|---|---|
| Endpoint1 | Endpoint | 14 | Low | 192.168.0.1 | Network Assets | Intel |
| Laptop1 | Laptop | 45 | Low | 192.168.0.2 | Network Assets | Buffalo |
| Endpoint2 | Endpoint | 25 | Low | 192.168.0.3 | Network Assets | |
| : | : | : | : | : | : | : |

リスク値：0(低)~100(高)


*CVEs: Common Vulnerabilities and Exposures: 共通脆弱性識別子

Monohakobi Technology Institute

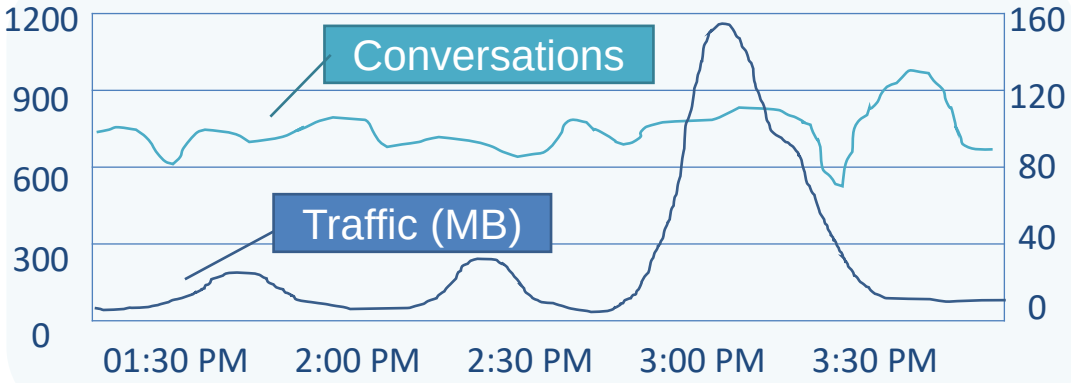
参考資料

NYK GROUP

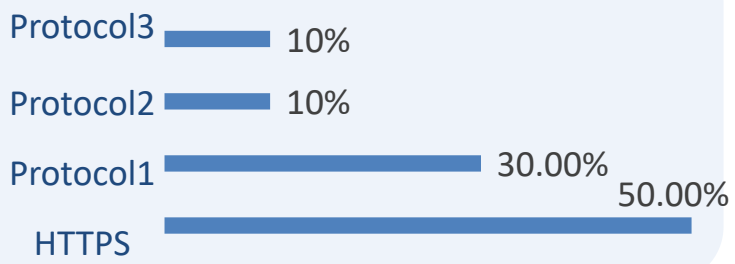
# 船舶のOT機器のモニタリング技術検証
## －通信状況の可視化－

通信状況の可視化

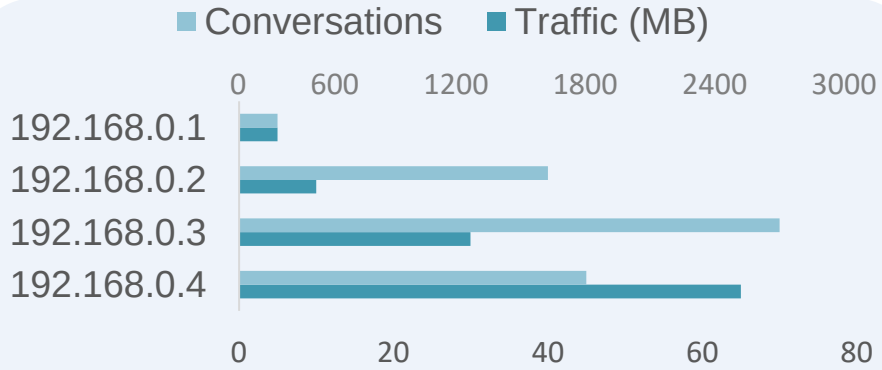
## トラフィック結果イメージ



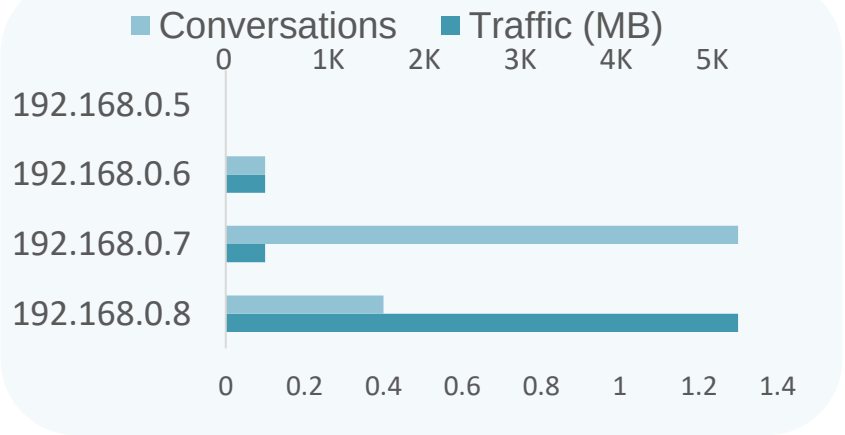

## プロトコルイメージ




## Top5送信元

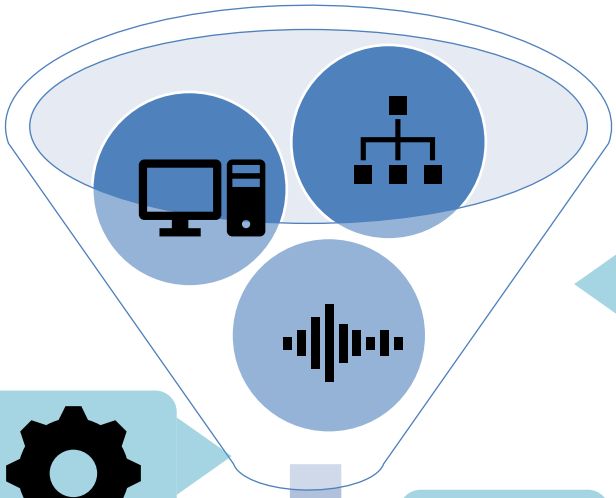



## Top5送信先



# 船舶のOT機器のモニタリング技術検証 ーポリシーの設定ー

ポリシーの設定・
イベントの検出・通知



モニタリングで
集まったデータ

ポリシーを設定

データとポリシーを元に、
**ポリシーに反するものを
イベントとして検出**

**イベントの通知**

- ✓ イベント詳細
- ✓ トリガーのポリシー
- ✓ ステータス|解決済・未解決
- ✓ イベントを確認すべき理由
- ✓ 推奨対応策

Monohakobi Technology Institute

参考資料

NYK GROUP

# 船舶のOT機器のモニタリング技術検証 ーイベント検出・通知ー

ポリシーの設定・
イベントの検出・通知

## イベント通知イメージ

| ID | 時間 | イベント | 重要度 | アセット | IP |
|---|---|---|---|---|---|
| 1 | 04:55 PM Mar 15, 2021 | Unauthorized Conversation | Low | Endpoint1 | 192.168.0.1 |
| 2 | 04:33 PM Mar 15, 2021 | Spike in Network Traffic | Medium | Laptop1 | 192.168.0.3 |
| 3 | 04:29 PM Mar 15, 2021 | New Asset Discovered | Low | Endpoint2 | 192.168.0.4 |
| 4 | 04:24 PM Mar 15, 2021 | Asset not seen for 1 hour | Low | Laptop2 | 192.168.0.8 |

**例**

- **イベントを確認すべき理由**

通信しているべき端末が通信していない場合、端末への通信経路が壊れているか端末が到達不可となっている。ネットワークが切断されたり、DoS攻撃が実行されている可能性がある。

- **推奨対応策**

端末へのpingまたはtracerouteを実行し、接続可能かどうかを検証し、接続不可の場合はどこで失敗するか確認する。一度に多くのアセットが消える場合は、障害が発生した可能性のある共通のネットワークコンポーネントがあるかどうか確認する。

# 船舶のOT機器のモニタリング技術検証 ー検証のまとめー

**アセットの管理**

ネットワーク内のアセットの**IPアドレスや機器情報**が**自動検出**され、**リスク値が自動算出**された。

**通信状況の可視化**

**通信量が多い送信元・送信先・プロトコル**が判明した。

**ポリシーの設定・イベントの検出・通知**

**ポリシーに該当するイベントの通知**を受け、**対処方法が推奨された。**

| IACS UR E26 | 検出されたイベント例 |
|---|---|
| ネットワーク接続の監視 | Unauthorized Conversation |
| 過度のトラフィックの監視及び検知 | Spike in Network Traffic |
| 権限を与えられていないデバイスの接続に対する監視又は防御 | New Asset Discovered |
| デバイス管理活動の監視及び記録 | Asset not seen for 1 hour |