船舶サイバーセキュリティ対策の取り組み

2022年11月24日

株式会社MTI　船舶物流技術グループ
若海　伽奈

目次

目次

1-1. 海事業界の現状

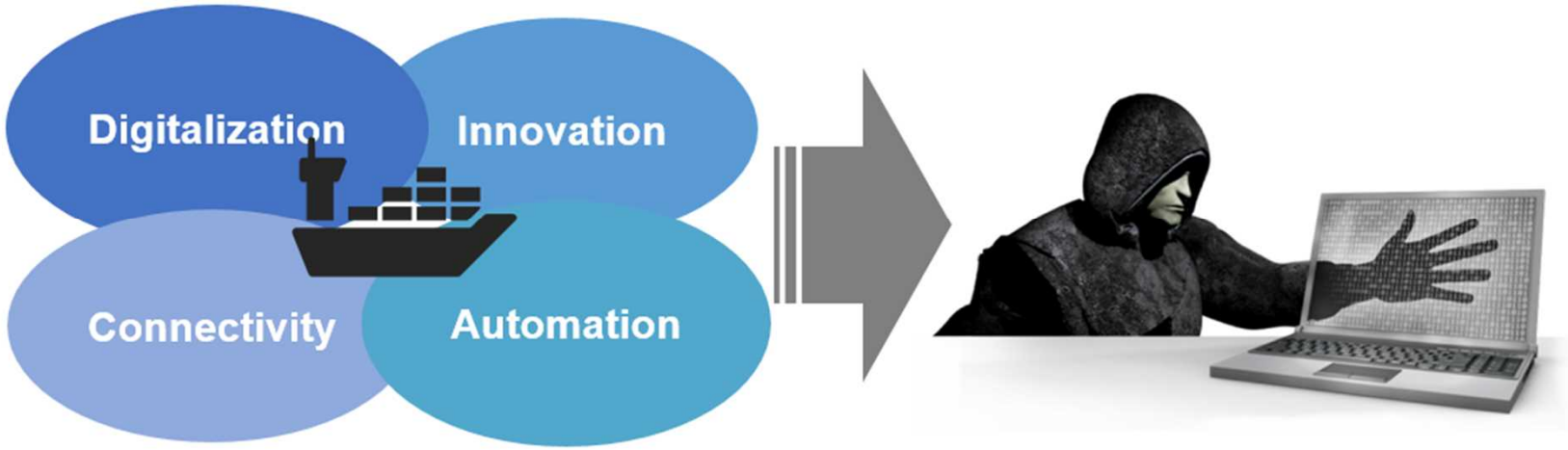
技術の発達により、船舶のサイバー攻撃のリスクが高まっている

✓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



1-2. 海事業界でのサイバー障害事例

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：陸上システム）

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

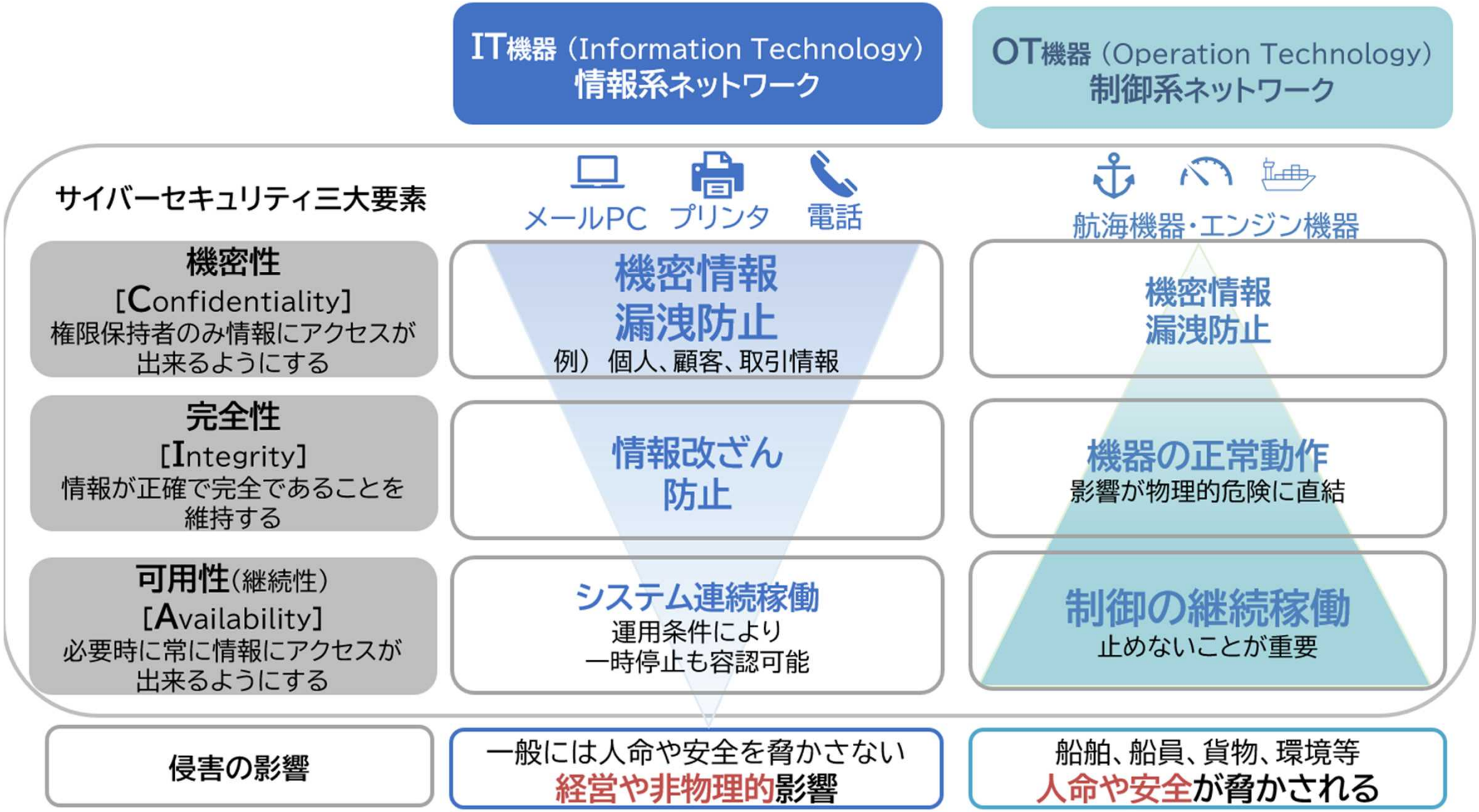
■OT機器（主な標的：船舶）

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 **G**lobal **N**avigation **S**atellite **S**ystems 全地球航法衛星システム。 GPS(米国)、準天頂衛星(日本)、 GLONASS(ロシア)、Galileo(EU)等の総称	バルト海 黒海 地中海東部中央部 スエズ運河 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 2022

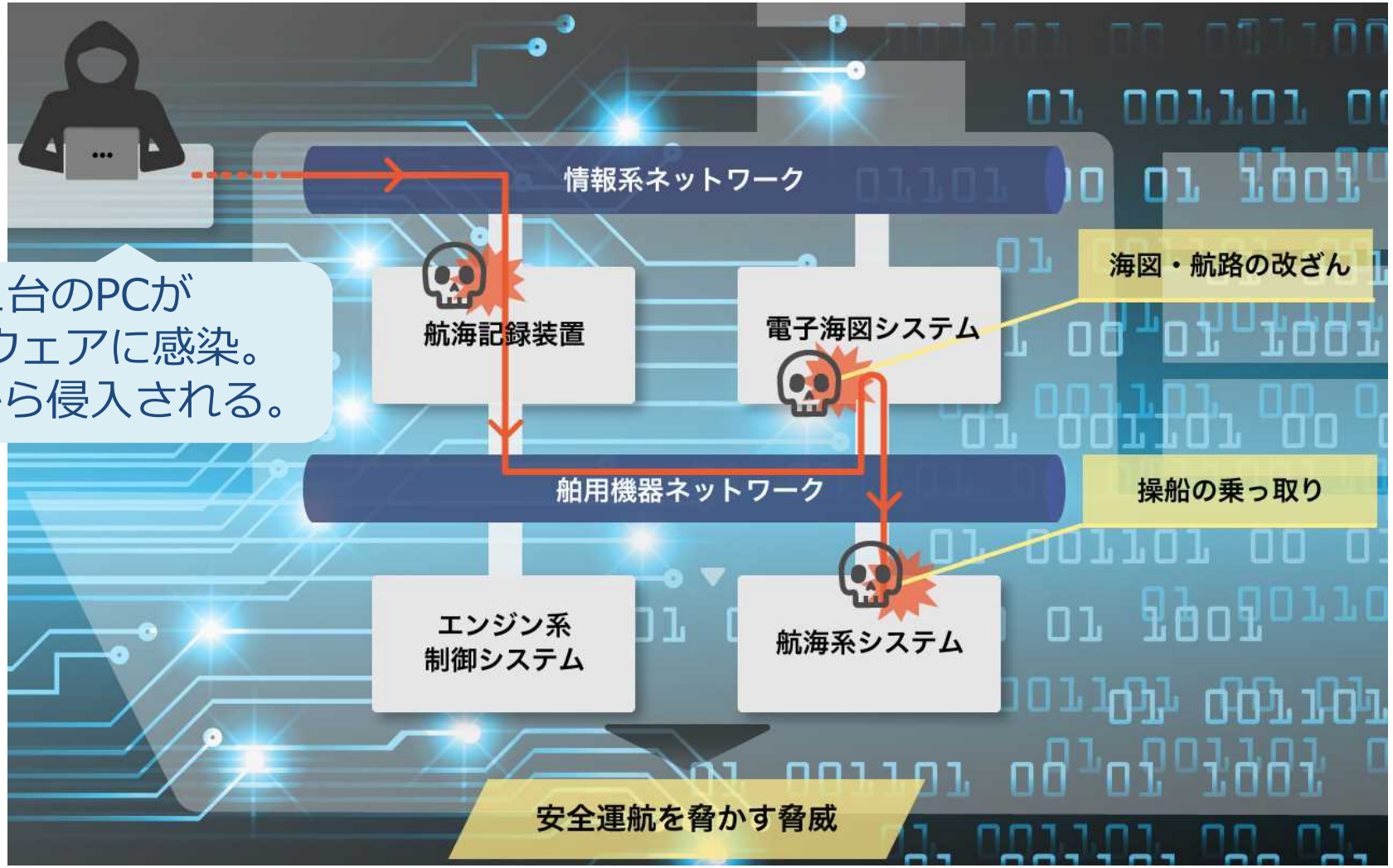
1-3. IT機器とOT機器

IT機器とOT機器は セキュリティの重要要素が異なる



1-4. 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

2-1. IMOや各国船級の議論

船舶サイバーセキュリティ対策の規定が強化している

2019 取得任意

各船級協会

「**ガイドライン**」や「**ノーテーション・認証**」発行

NYK) 複数のLNG船で、ClassNKやBVのサイバー認証取得(2019.12)

2021 強く推奨

IMO MSC98

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

NYK)
サイバーリスク管理ポリシー策定、
インハウス各管理会社でSMSの下リスク管理・対策実施

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: Unified Requirements

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

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

2-2. IACS UR E26･E27概要

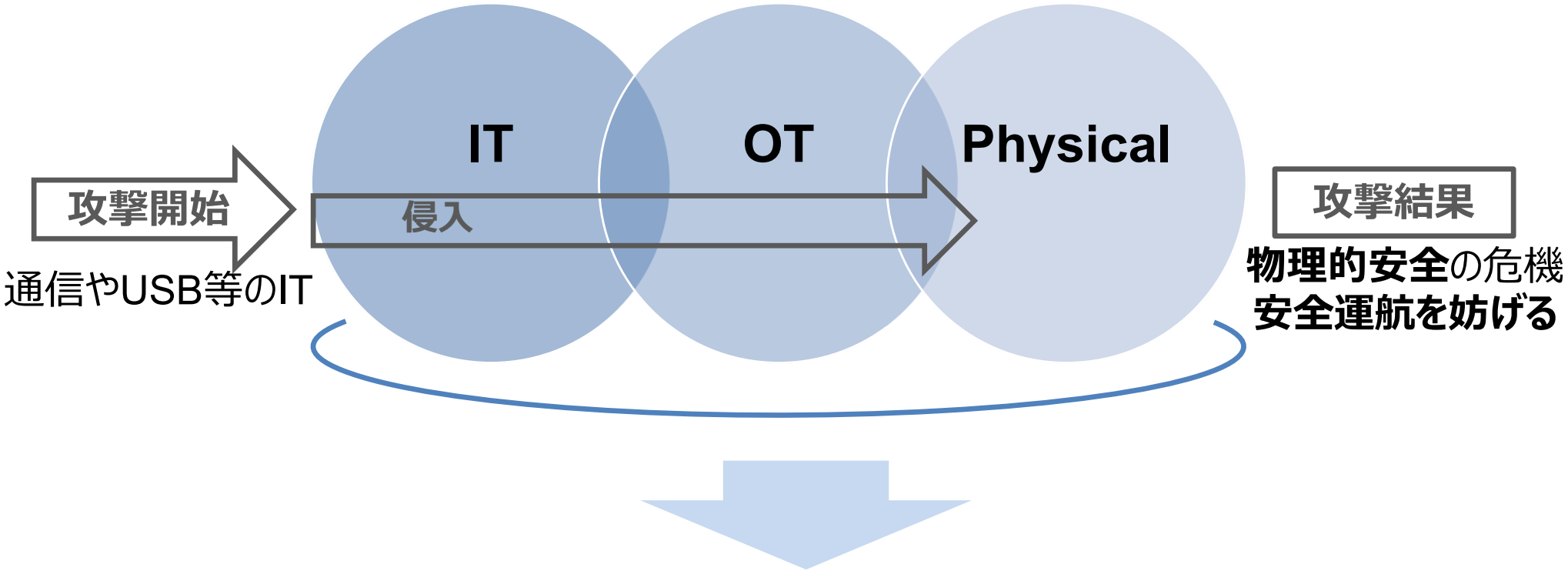
	E26 船舶のサイバーレジリエンス	E27 船上のシステム及び機器のサイバーレジリエンス
要件	**船舶全体**	**個々の船上機器**
目的	船舶の**設計から運航まで**の全工程で、**船舶のネットワークにITとOT両機器が安全に統合される**ことを目指し、**特定-防御-検知-対応-復旧**の側面からセキュリティ要件を定義。	**機器ベンダ**により**システムの整合性を担保**するための要件を定義。 主に制御システム向け規格のIEC62443-3-3,IEC62443-4-1を引用
構成	1. 導入 2. 用語定義 3. ゴール及び要件の構成 **4. 要件(特定-防御-検知-対応-復旧)** 5. 機能評価とテストプラン 6. 本要件適用対象外とする際のリスク評価 Annex.アクションと提出書類の要約	1. 一般 2. セキュリティの考え方 3. 船級協会への提出図書 **4. システムに関する要件** **・セキュリティ要件** **・追加要件** **5. 製品の設計・開発要件** Annex. 関連UR・参考文献

目次

3-1. 守るべき対象

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**



「Physical(物理的)安全対策」とセットでの対策が必要。

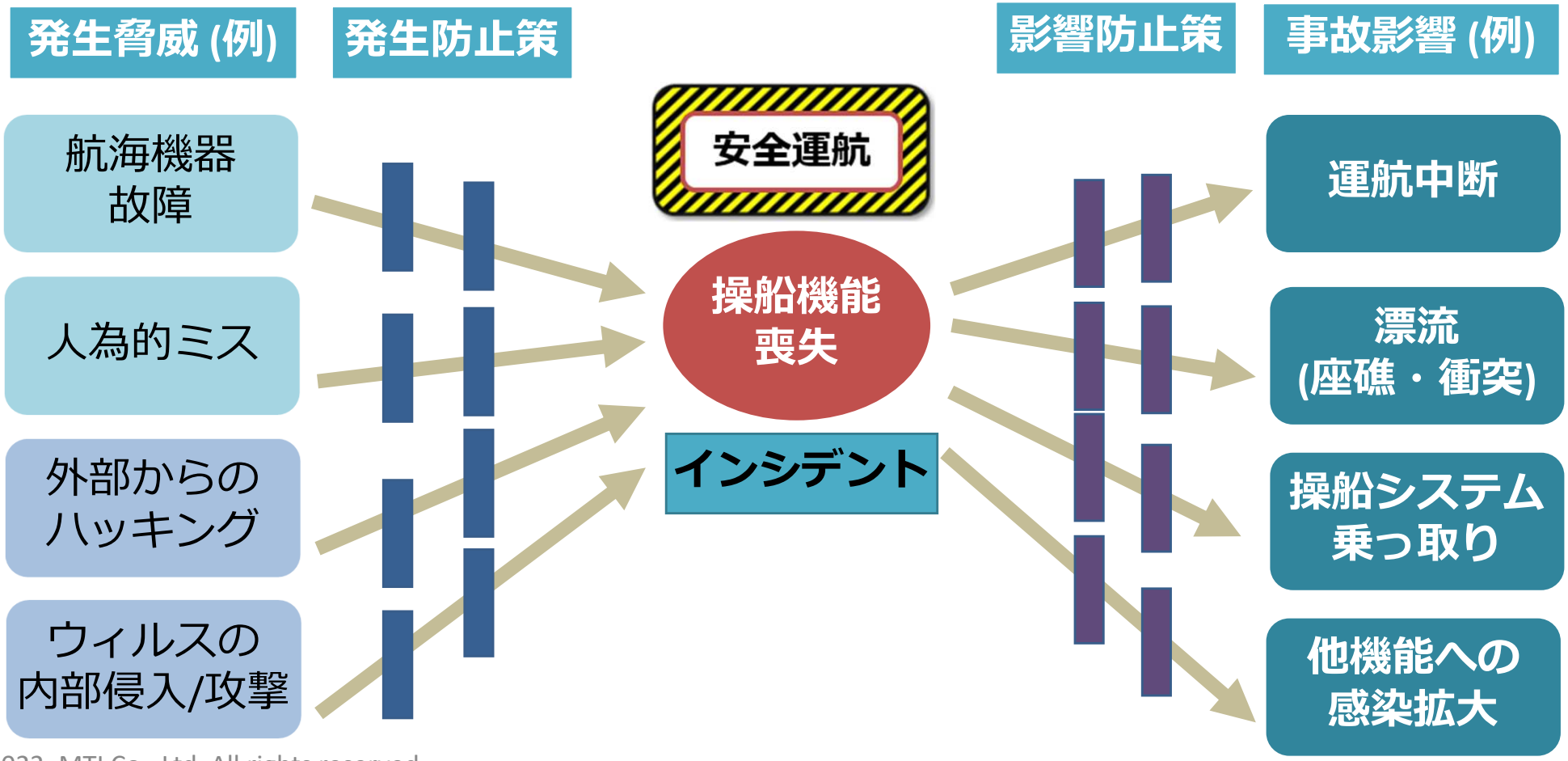
3-2. 「物理的な安全対策」と「サイバー対策」の関係

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



3-3. 今後の対策に更に必要となるもの

「特定・防御」だけでなく「検知」「対応」「復旧」が重要

特定
防御
検知
対応
復旧

1

船舶のサイバー**脅威**を適切に**把握**し、
それらをフリート全体で**統合的に監視**し、
インシデント発生前に**早期検知・予防**する**仕組み**

2

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**教育**

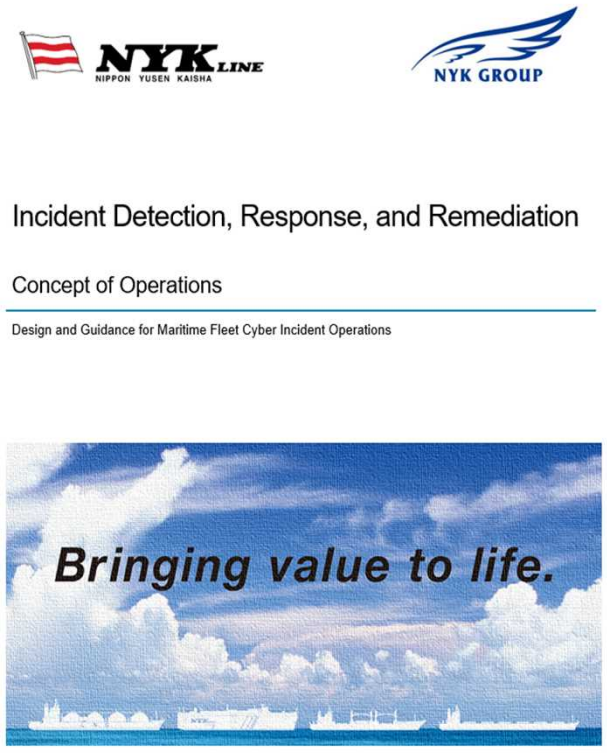
目次

4-1.船舶サイバーセキュリティ対応のConOps作成

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

4-2. ConOpsに基づいた対策の開始

組織、プロセス、技術の側面からの強化を実施中

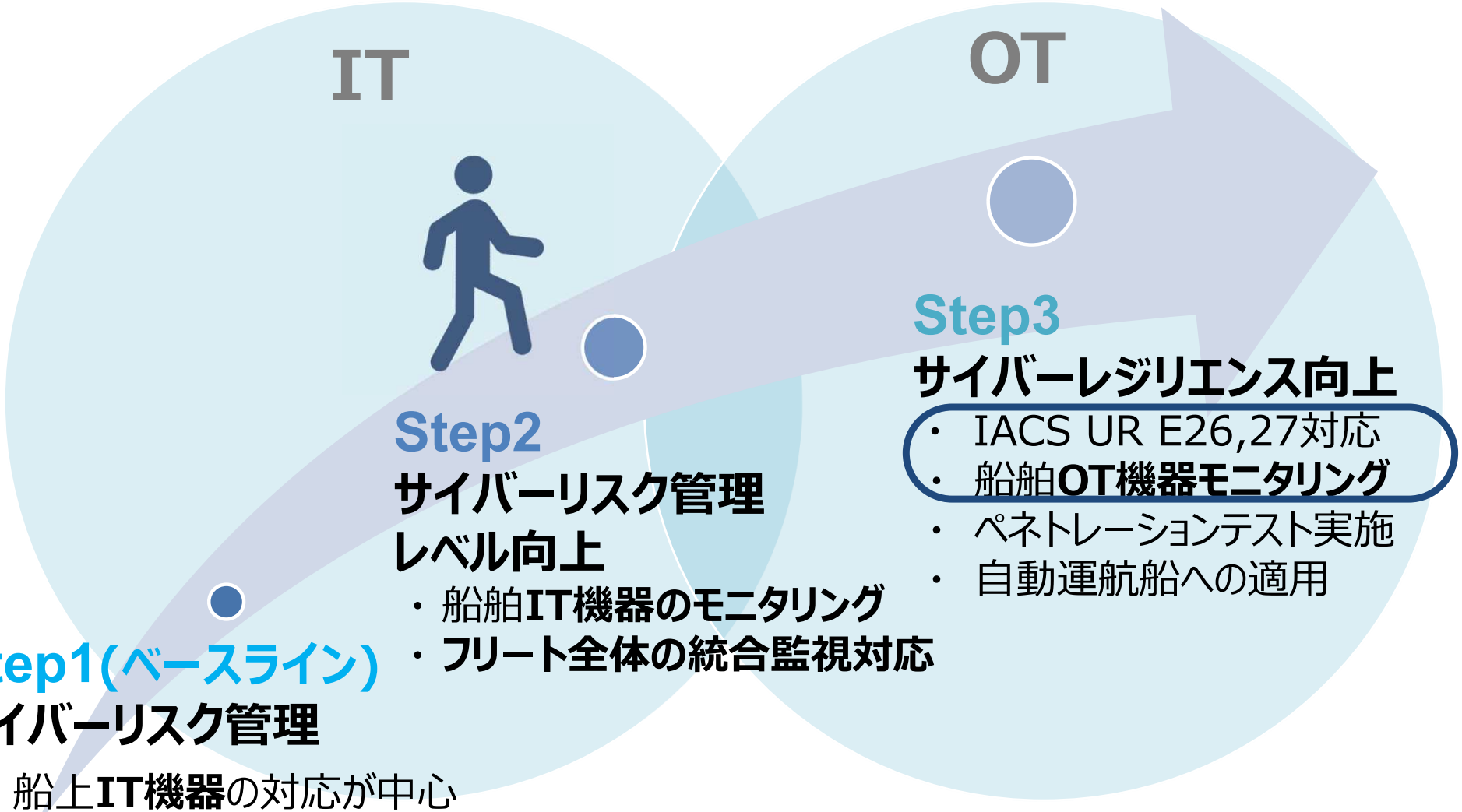
・船舶サイバーインシデント対応**組織、人員配置の強化**
・船舶サイバー**監視組織の構築**

・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**ツールの検証

4-3.船舶サイバーセキュリティ対策の現状と今後

ITの対策を進めつつ、対策のOTへの展開準備を進める



4-4. IACSのモニタリングの要求

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

4-5.OTモニタリングツールの検証の実施

技術

検証概要

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** *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 2. ネットワークマップの自動生成 3. ポリシーの設定、イベントの検知・通知 4. 通信状況の可視化 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

4-6.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	
:	:	:	:	:	:	:

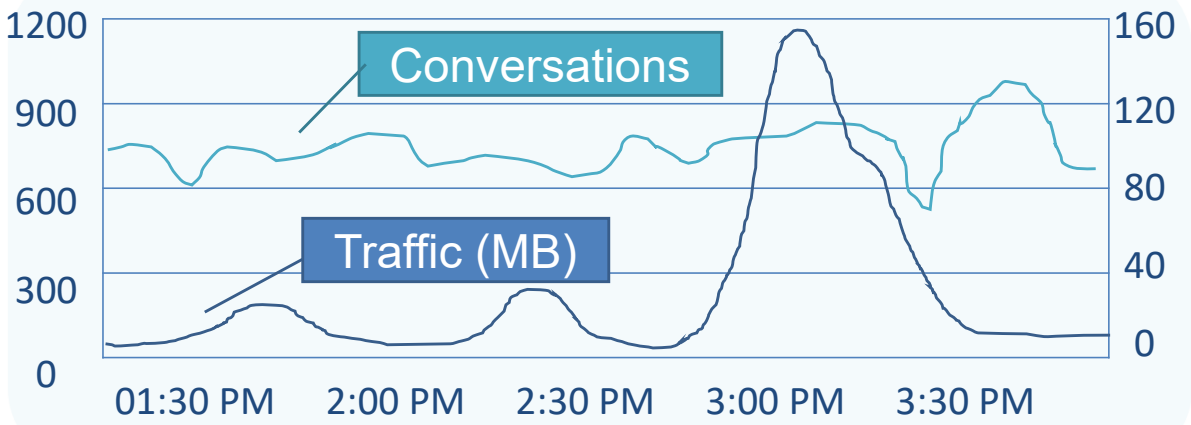
リスク値：0(低)~100(高)

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

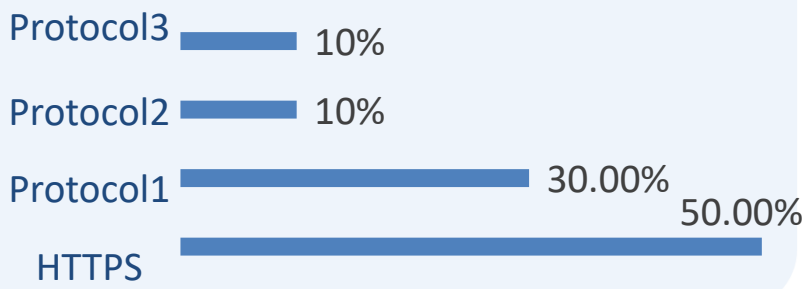
4-6.船舶のOT機器のモニタリング技術検証 －通信状況の可視化－

通信状況の可視化

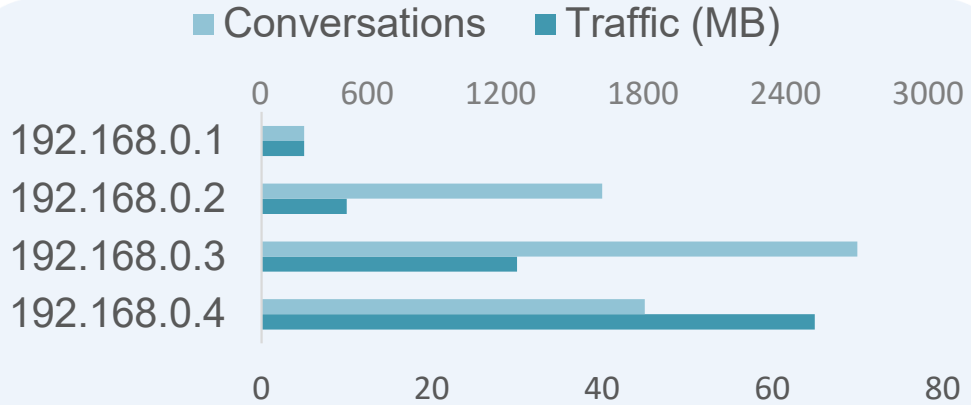
トラフィック結果イメージ



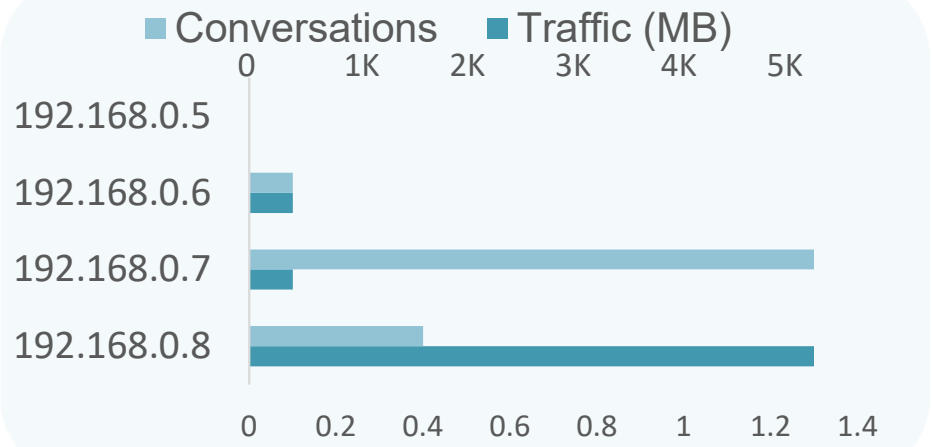
プロトコルイメージ



Top5送信元

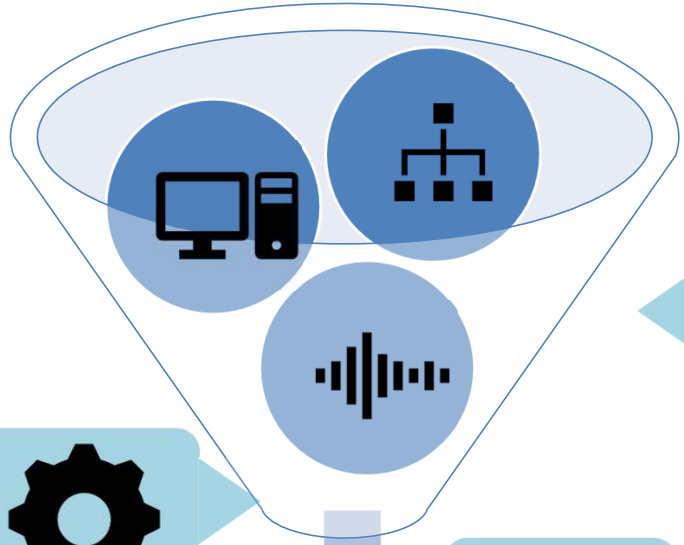


Top5送信先



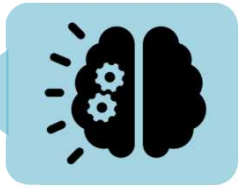
4-6.船舶のOT機器のモニタリング技術検証 ーポリシーの設定ー

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

4-6.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。

4-6.船舶のOT機器のモニタリング技術検証 ―検証のまとめ―

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

目次

5-1. 発表内容のまとめ

1. 船舶サイバーセキュリティのガイドラインや規制の動向

✓ 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。

2. 船舶運航のサイバーリスク管理

✓ 船舶への攻撃は**ITから始まり、OT機器へ侵入し、安全運航への影響をもたらす。**

✓ 安全運航を守るためには、**OT機器を守ることが重要。**

✓ **サイバーセキュリティ対策は物理的な安全対策と共に取り組む**必要がある。

3. 船舶サイバーレジリエンス向上のためのNYKでの取り組み

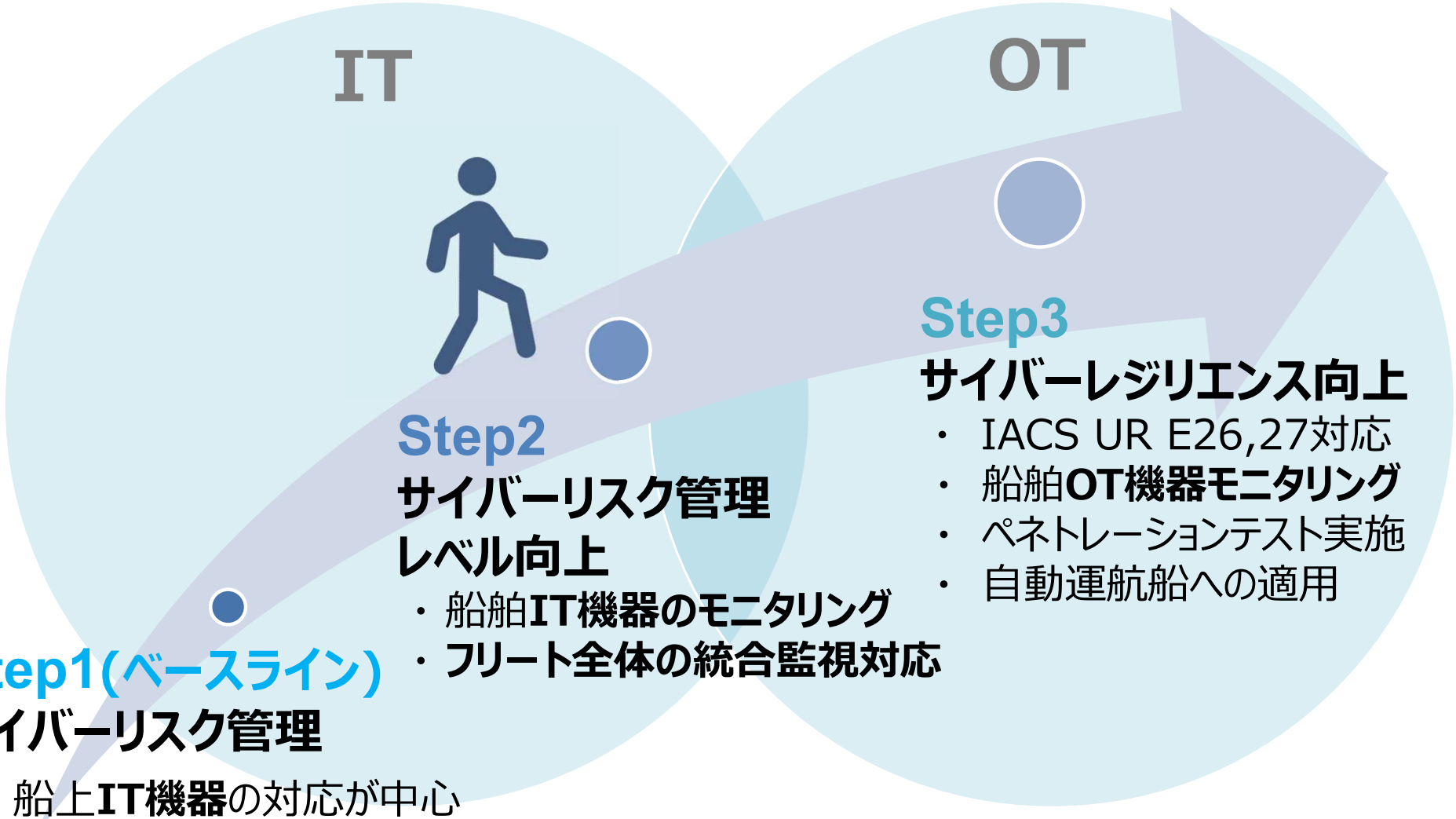
✓ 組織・プロセス・技術を網羅したConOpsを作成し、 ConOpsに基づいた対策を構築中。

✓ IACS UR E26の要件に含まれるOT機器のモニタリングを、研究開発案件として船舶の操船機器を模擬した環境で検証。

→**検知されるべき通信が検知**され、**モニタリングをしていなければ気がつくことが出来なかった異常が検知された**ことを確認した。

5-2.船舶サイバーセキュリティ対策の現状と今後

ITの対策を進めつつ、対策のOTへの展開準備を進める



ご清聴どうもありがとうございました。