海運における
船舶サイバーセキュリティ対策について

2021年2月12日

株式会社MTI　船舶物流技術グループ
柴田　隼吾

目次

日本郵船グループについて

- 会社名：**日本郵船株式会社**（Nippon Yusen Kabushiki Kaisha）
- 代表取締役：長澤 仁志
- 設立：1885年 (明治18年) 9月29日　　創業136年目
- 本社：〒100-0005 東京都千代田区丸の内 2-3-2 郵船ビル
- 従業員数：34,857名 (2020年3月末時点)
- 売上高：16,683億円 (2019年度)
- URL：http://www.nyk.com/
- 事業内容：

一般貨物輸送事業

- 定期船事業（コンテナ船部門／ターミナル関連部門）
- 航空運送事業
- 物流事業

不定期専用船事業

- ドライバルク輸送部門
- エネルギー輸送部門
- 自動車輸送部門

その他事業

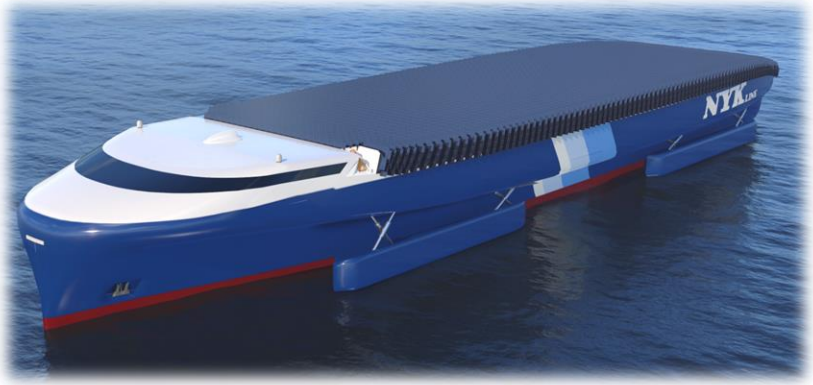
- 不動産業
- その他の事業

日本郵船グループの運航船（所有/運航）

ＭＴＩ（Monohakobi Technology Institute）について

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**
- 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：69名 (2020年4月1日現在)
- 資本金：9,900万円
- 株主：日本郵船株式会社 (NYK LINE)
- 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



<u>シンガポール支店</u>

- 1 Harbour front Place #13-01,
  Harbourfront Tower One
  Singapore 098633

<u>YOKOHAMA LAB</u>

(輸送環境実証実験施設)

- 〒235-0033 神奈川県横浜市磯子区
  杉田5-32-84

Smarter ship and operation in NYK/MTI

Now → Future: OIL → LNG → HYDROGEN

Ship (Hardware)

- Alternative Marine Power
- Wind Resistance Reduced *MT-COWL*
- Super Eco Ship2030
- 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*
- LNG-Fueled PCTC Delivery in 2016
- Super Eco Ship 2050 carbon free concept ship
- Air Lubrication System *YAMATO, YAMATAI*
- Innovative Air Lubrication System *SOYO*
- Electronic Controlled Engine
- Improved Governor Controller
- *MT-FAST*
- Hybrid Electric Power Supply *Auriga Leader*
- LNG Bunkering Vessel Delivery in 2016
- Unmanned Autonomous Ship Trial Project (MEGURI)

Operation (Software)

- MTI Founded
- NYK's own safety and Environment standard *NAV9000*
- Prediction of Current
- Fuel Consumption Indicator *FUELNAVI*
- 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

目次

1）海運における船舶サイバーリスクの高まり

- ✓ VSAT衛星通信技術の発達により、船舶の**インターネット常時接続**が普及
- ✓ 船舶の運航データを陸上でモニタリングするなど、**船陸間のデータ共有が急増**
- ✓ 一方で、舶用機器のコンピューター化や、船陸通信の接続に伴い、船舶の内外からのウイルス感染、不正アクセスといった**サイバー攻撃に晒されるリスクが高まる**

➡ **2017年6月に開催された、国際海事機関（IMO）海上安全委員会 において、船舶のサイバーリスク対策は、「海上人命安全条約（SOLAS条約）」における国際安全コード（ISMコード）に基づき、2021年1月以降から船主・運航者の“安全管理システム(SMS)にて対応すること”が強く推奨される。**

2．海運における船舶サイバーリスクとは

船舶サイバーセキュリティで守るべき対象は、

安全運航を支える ”OT機器”

※OT機器を守る＝”乗っ取り“や”運航不能“を防止して、
船の運航に関する各機能の正常動作を維持する

■その他にも、守るべき対象はさまざま：

例） 船上のPCや、そこに含まれる情報：**損傷、改変、悪用**からの保護

船陸間衛星通信／無線通信：**傍受、なりすまし、通信妨害**からの保護　など

■**船舶に対するサイバー攻撃の手段：**

・**攻撃は、メール添付や、不正URL、USBメモリ経由**が主流

・OTシステムの乗取り/機能停止以外にも、**データ漏洩、破壊、改ざん**

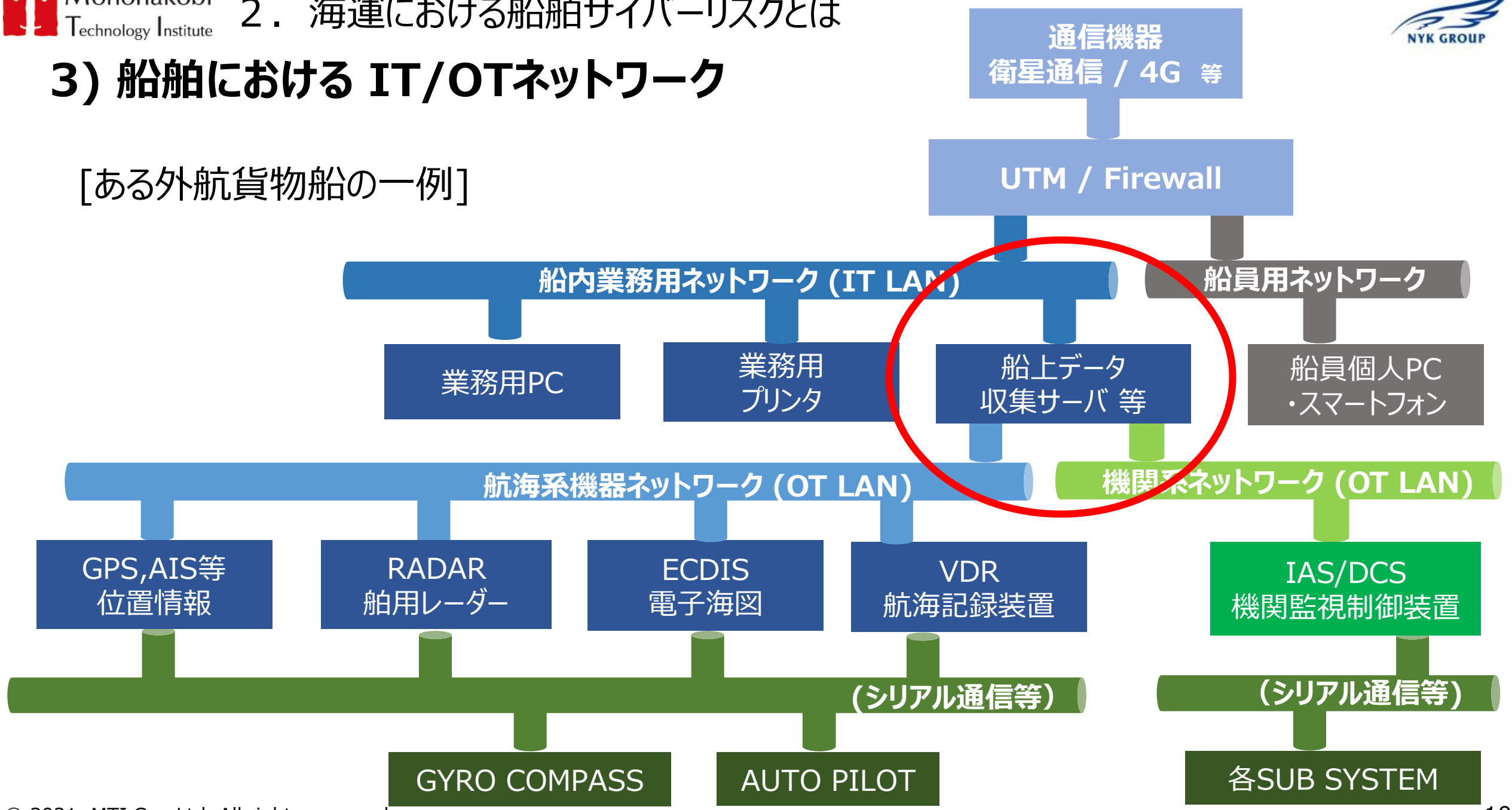
攻撃例：マルウェア、ランサムウェア、GPS信号なりすまし

2) 船舶運航とサイバーセキュリティ

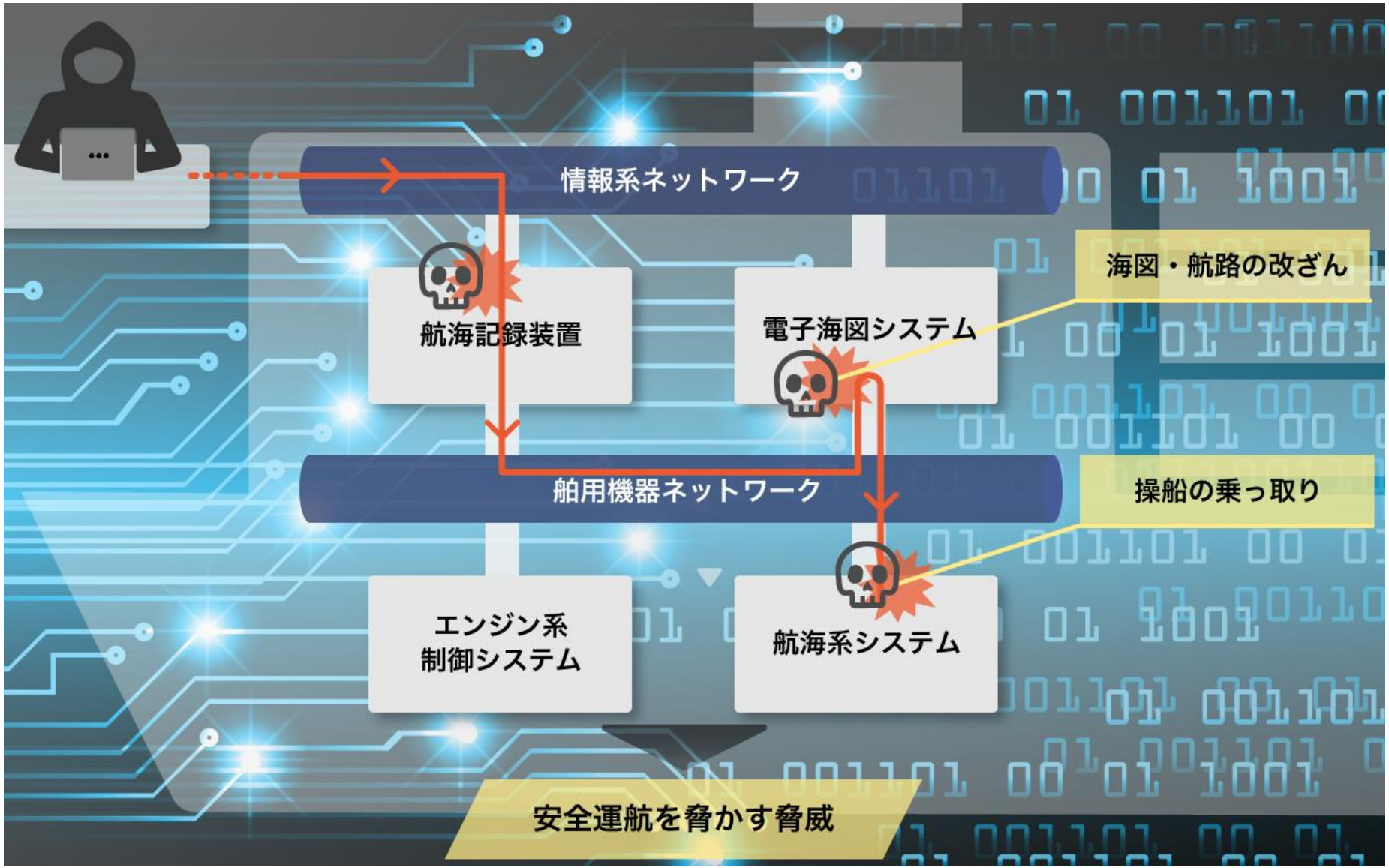
	IT機器 （Information Technology）	OT機器 （Operation Technology）
サイバーセキュリティ ３大要素	メールPC、業務用PC、プリンタ および船内情報ネットワーク　など	航海機器・エンジン機関 および制御ネットワーク　など
機密性 [**C**onfidentiality]	・**情報の漏洩防止が重要** 例）個人、顧客、貨物情報保護 データ暗号化	・データ漏洩の影響度は低い 例）舶用機器の設定値 運航状態データ
完全性 [**I**ntegrity]	・**運航や貨物情報の改ざん防止** ・情報整合性の保持が重要	・**運航機器の正常動作が重要** ・**運航の安全性が最優先** ・リスクの影響が衝突や座礁など 物理的危険に直結する 可能性が高い
可用性（継続性） [**A**vailability]	・システムの一時的な停止が 運用要件により容認できる ・運用のリアルタイム性が低い ・緊急対応の重要性は低い	・**運航機能の継続稼働性が重要** ・機器再起動は運航状況により 許容できない ・陸上からの支援なしにも 緊急対応ができることが重要

3) 船舶における IT/OTネットワーク

[ある外航貨物船の一例]



4) 船舶OT機器へのサイバー攻撃イメージ



5) 船舶へサイバー攻撃事例

①操舵機器のハッキングによる操船乗取り

✓2017年2月、紅海付近を航行するコンテナ船が**約10時間にわたり操船システムを乗っ取られる。**

✓**“突然、船の操縦ができなくなった。航海システムは完全にハッキングされていた。**”と、関係者は語った。

✓**外部のIT専門家と連携し、**何時間もの対応の結果、なんとか乗っ取りをブロックすることが出来た。

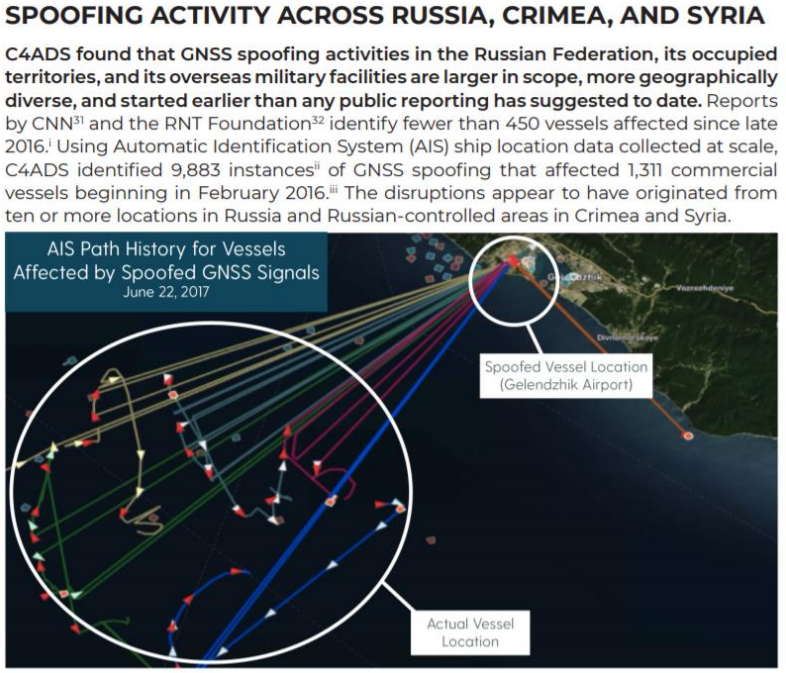
✓原因はいまだ不明ではあるが、攻撃者は海賊であり、船を襲いやすい場所に誘導する目的だったとの見方が有力とも。

出典) https://safetyatsea.net/news/2017/shipping-must-confront-onboard-systems-cyber-vulnerabilities/

5) 船舶へサイバー攻撃事例

②GPS信号の改ざん(スプーフィング)

- ✓黒海付近では、この数年間で**1万件以上の船舶でのGPS位置情報の改ざん**が発生
- ✓**1000隻以上の商船の航行に影響**
- ✓米国シンクタンク(C4ADS)は、**ロシア軍による GPSスプーフィング行為が原因**であると報告

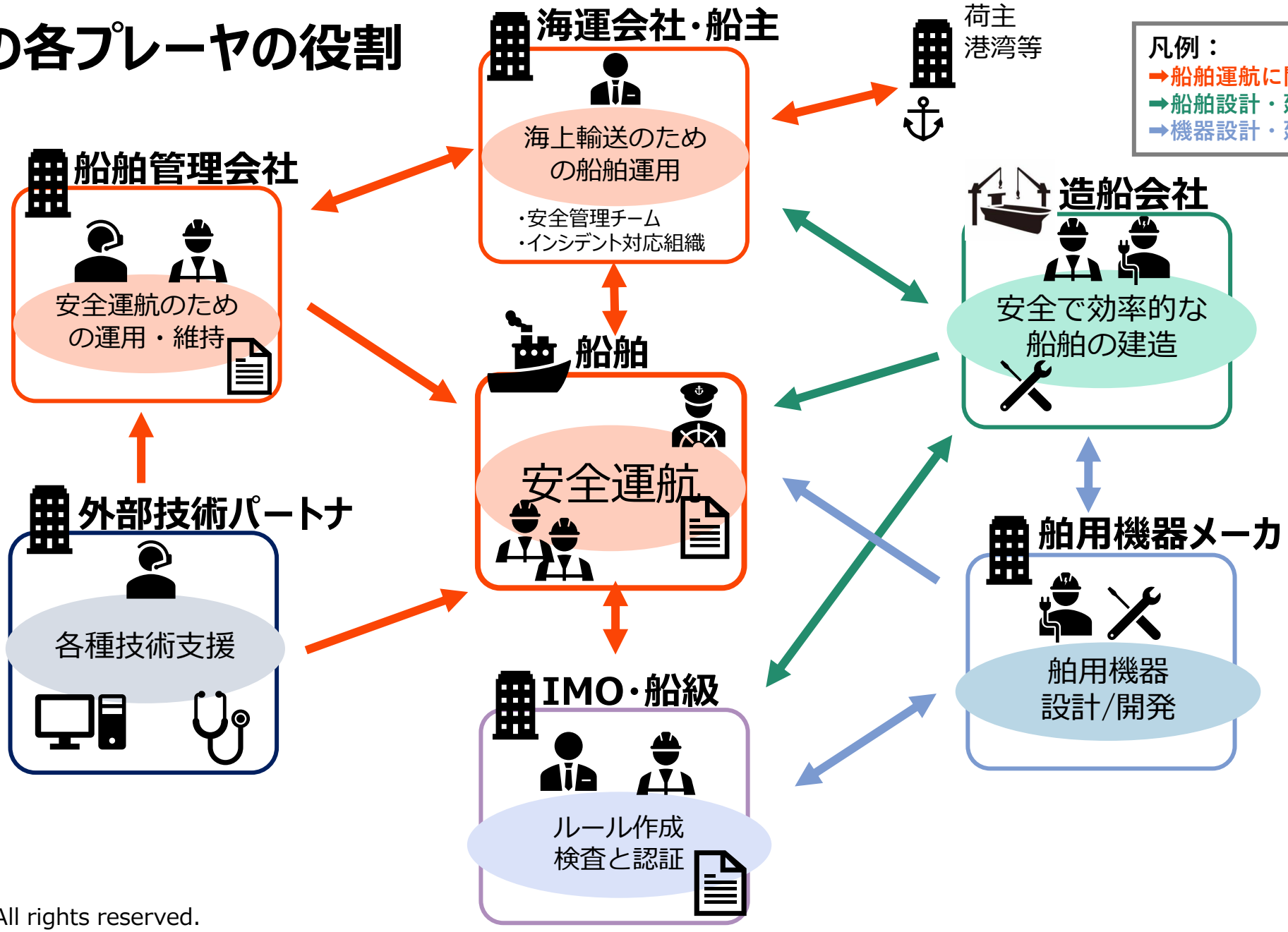


出典）Above US ONLY STARS, The Center for Advanced Defense Studies
米国高等国防研究センター（C4ADS），2019年3月発行

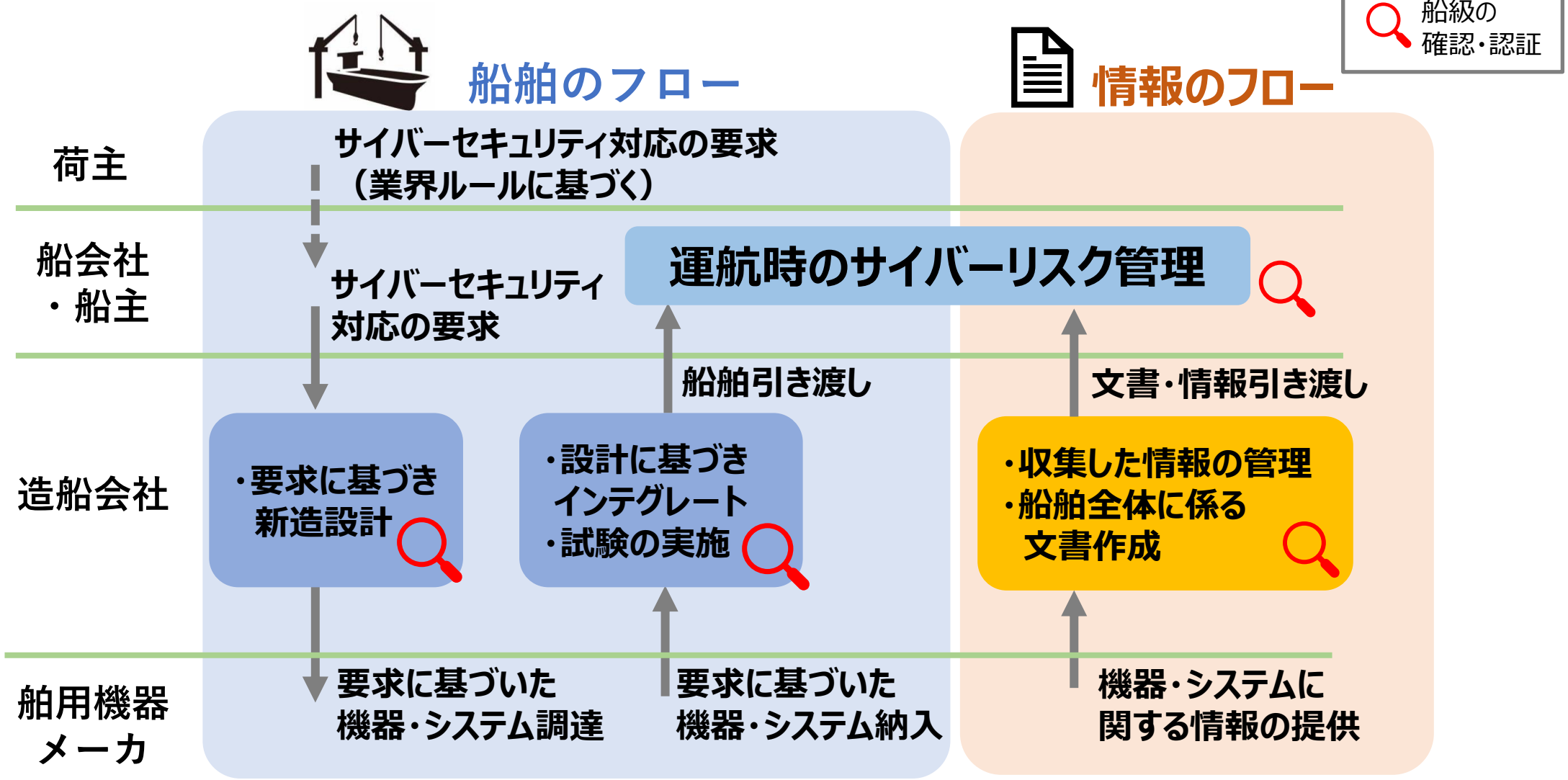
目次

3．業界内での議論と対応

1) 海運の各プレーヤの役割



1) 海運の各プレーヤの役割



3． 業界内での議論と対応

凡例：
- 運用（船社）に関係
- 設計・建造（造船所）に関係
- 設計・建造（メーカー）に関係

NYK GROUP

2) IMO･業界団体･船級のガイドラインや認証

2021年1月弊社調べ

		2016	2017	2018	2019	2020	2021
IMO /国際海事機関			● MSC-FAL.1/Circ.3の承認【6月】 ● MSC.428(98) の採択【6月】		“強く推奨” →		● SMSでのサイバーリスク管理【1月～】
IACS /国際船級協会連合			● UR E-22 Rev.2発行【6月】		● 12 Recommendation 公開【11月】	統合 →	● N.166に 統合【4月】 ● N.166修正版公開【7月】 ＊統一規則化の見込み
BIMCO /ボルチック国際海運協議会			● ガイドライン 第1版発行【1月】 改訂 →	● ガイドライン 第2版発行【7月】 →	● ガイドライン 第3版発行【12月】 →		● ガイドライン 第4版発行【12月】
主要な船級協会	ABS /アメリカ		● CS Notation 発行【7月】		● CS Ready Notation 発行【6月】	● CS for Equipment Manufacturers 発行【10月】	
	BV /フランス			● SYSCOM発行【10月】 ● SYSCOM発行【10月】	● CYBER MANAGED Notation発行【12月】 →		● CYBER (MANAGED) (SECURE) Notation発行 ● CYBER (MANAGED) (SECURE) Prepared Notation発行【9月】
					● CYBER SECURE Notation発行【12月】 →		
	DNV-GL /ドイツ・ノルウェー		● RP: Cyber Security Resilience Management発行【12月】	● CP-0231発行【1月】 →	● Cyber Secure (basic) Notation発行【7月】 →	● CP-0231改訂【3月】 ● Cyber Secure Notation発行【2月】	
					● Cyber Secure (advanced) Notation発行【7月】 →	● Cyber Secure (Essential) (Advanced)Notation発行	
	LR /イギリス		● Cyber Security Maturity Framework発行【7月】 ● 型式認証 Network-related devices 発行【9月】 ● ShipRight発行【12月】		● Cyber Secure (basic)Notation発行【7月】		
	ClassNK /日本				● マネジメントガイドライン発行【3月】 ● マネジメント認証【12月】 ● デザインガイドライン発行【2月】 →		● デザインガイドライン第2版発行【7月】
					● ソフトウェアガイドライン発行【5月】		

3．業界内での議論と対応

ガイドラインや規則など、**要件(Plan)**の作成は進み、各事業者は、いかに要件を満たす対応を**実施(Do)**するかを対策中。しかし、**検証(Check)**の仕組みや体制の整備は道なかば

		Security by Design		Security Management
	フェーズ	舶用機器製造	船舶建造	船舶運用
	主担当	舶用機器メーカ	造船会社	船社
改善(ACT)	要件(Plan)	IACS No.166 “Recommendation on Cyber Resilience”(2020.4) 各国船級による舶用機器向けガイドライン・認証 船技協 舶用機器向けガイドライン作成中 (2020年度)	各国船級による新造船向けガイドライン・認証 船技協 CyberResilient Shipガイドライン発行 (2020.3)	IMO MSC-FAL.1/Circ.3 (2017) BIMCOガイドライン (2018.11) 各国船級 船主向けガイドライン認証 船技協 サイバーリスク管理テンプレート発行 (2019.3)
	実施(Do)	舶用機器メーカ向けガイドライン等に基づき対応	Cyber-Resilient shipガイドライン等に基づき対応	CSMSテンプレートに基づき、SMSでの対応を実施 (2021年1月～)
	検証(Check)	舶用機器・システムに対する検証・テスト手法の整備が必要	船舶全体のシステムや、各ファンクションのサイバー耐性を検証する手法の整備が必要	2021年1月以降の最初の適合証書の年次検査で実施 運航時におけるサイバーインシデントへの対応演習

凡例：各国船級が実施／業界団体が実施／整備中のもの

*船技協 ：
(一財)日本船舶技術研究協会

3．業界内での議論と対応

3) 船舶運用での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を実現

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：

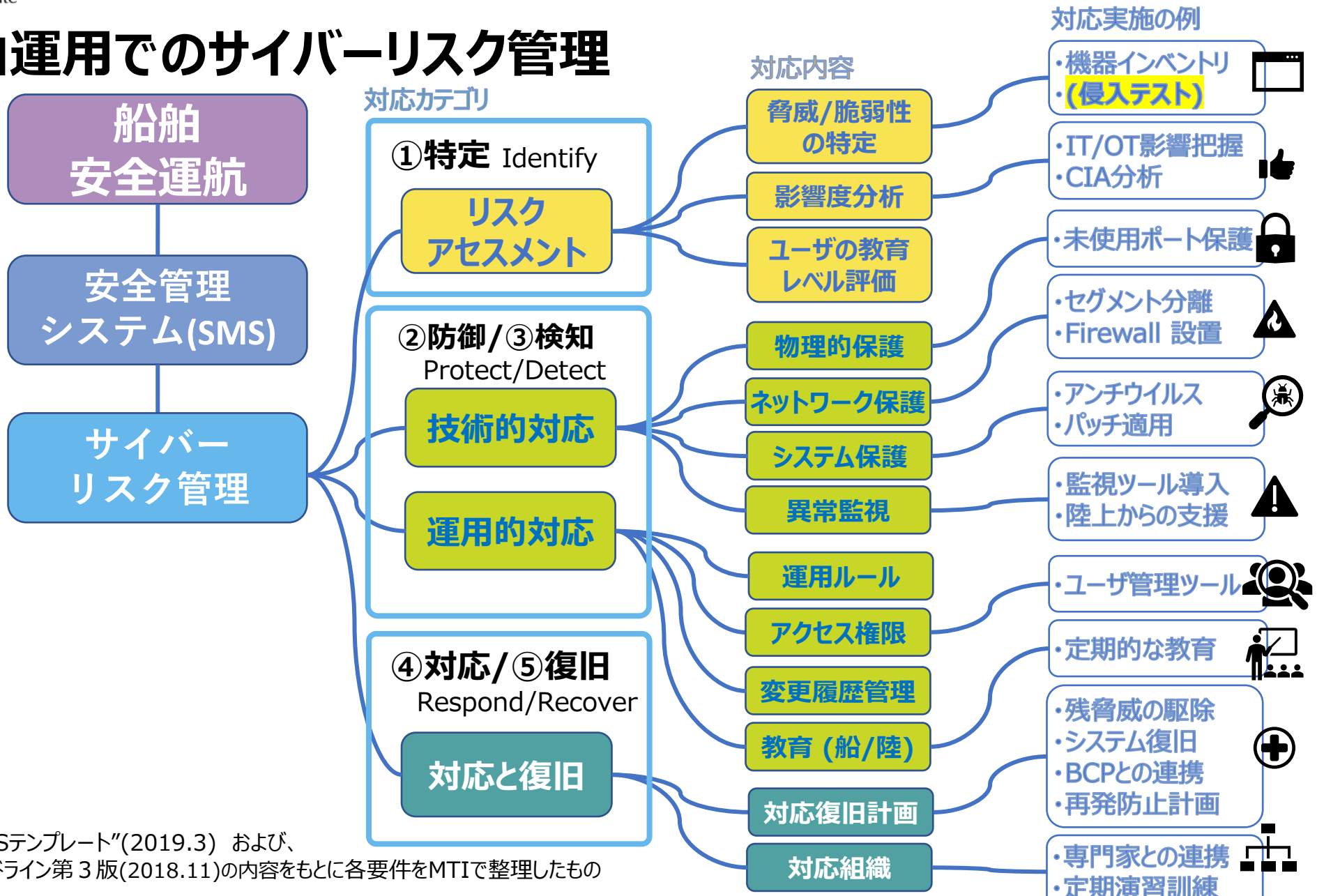
NIST(*1) Cybersecurity Framework
“5つの対応カテゴリ” に整理し改善することが多くのガイドラインでも推奨されている

*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．業界内での議論と対応

3) 船舶運用でのサイバーリスク管理

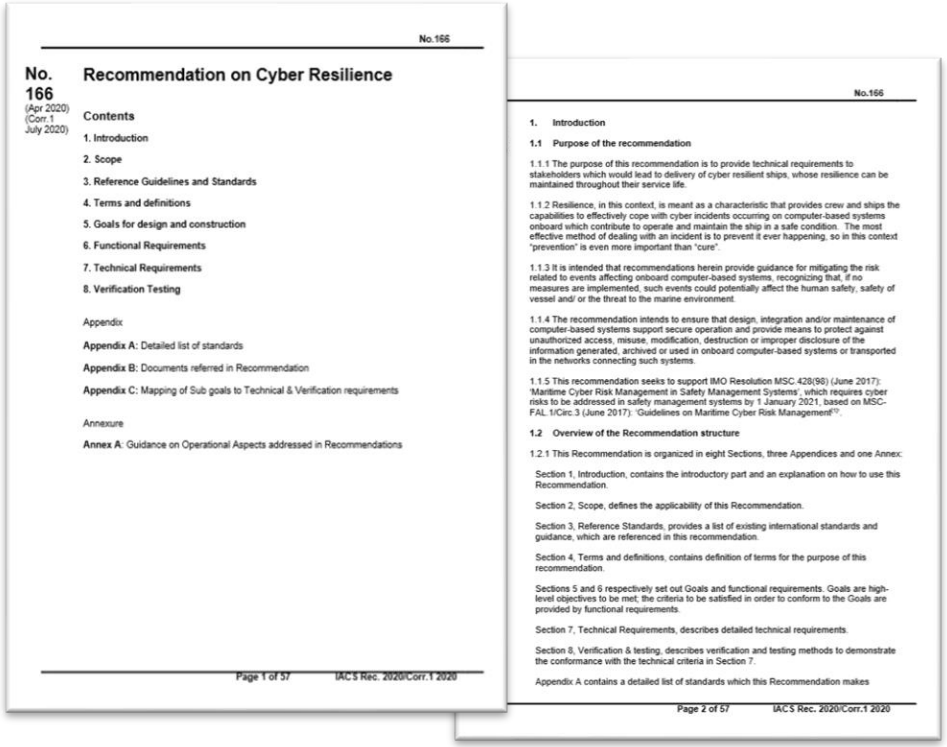


※船技協 “SMSテンプレート”(2019.3) および、
BIMCOガイドライン第３版(2018.11)の内容をもとに各要件をMTIで整理したもの

4) 船舶建造におけるサイバーレジリエンス向上

国際船級協会連合(IACS) 2020年4月発行
Recommendation on Cyber Resilience
(No.166)

目次



No.166

No. 166 (Apr 2020) (Corr.1 July 2020)

Recommendation on Cyber Resilience

Contents

Page 1 of 57 IACS Rec. 2020/Corr.1 2020

No.166

1. Introduction

1.1 Purpose of the recommendation

1.1.1 The purpose of this recommendation is to provide technical requirements to stakeholders which would lead to delivery of cyber resilient ships, whose resilience can be maintained throughout their service life.

1.1.2 Resilience, in this context, is meant as a characteristic that provides crew and ships the capabilities to effectively cope with cyber incidents occurring on computer-based systems onboard which contribute to operate and maintain the ship in a safe condition. The most effective method of dealing with an incident is to prevent it ever happening, so in this context "prevention" is even more important than "cure".

1.1.3 It is intended that recommendations herein provide guidance for mitigating the risk related to events affecting onboard computer-based systems, recognizing that, if no measures are implemented, such events could potentially affect the human safety, safety of vessel and/ or the threat to the marine environment.

1.1.4 The recommendation intends to ensure that design, integration and/or maintenance of computer-based systems support secure operation and provide means to protect against unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard computer-based systems or transported in the networks connecting such systems.

1.1.5 This recommendation seeks to support IMO Resolution MSC.428(98) (June 2017): 'Maritime Cyber Risk Management in Safety Management Systems', which requires cyber risks to be addressed in safety management systems by 1 January 2021, based on MSC-FAL.1/Circ.3 (June 2017): 'Guidelines on Maritime Cyber Risk Management'[1].

1.2 Overview of the Recommendation structure

1.2.1 This Recommendation is organized in eight Sections, three Appendices and one Annex:

Section 1, Introduction, contains the introductory part and an explanation on how to use this Recommendation.

Section 2, Scope, defines the applicability of this Recommendation.

Section 3, Reference Standards, provides a list of existing international standards and guidance, which are referenced in this recommendation.

Section 4, Terms and definitions, contains definition of terms for the purpose of this recommendation.

Sections 5 and 6 respectively set out Goals and functional requirements. Goals are high-level objectives to be met; the criteria to be satisfied in order to conform to the Goals are provided by functional requirements.

Section 7, Technical Requirements, describes detailed technical requirements.

Section 8, Verification & testing, describes verification and testing methods to demonstrate the conformance with the technical criteria in Section 7.

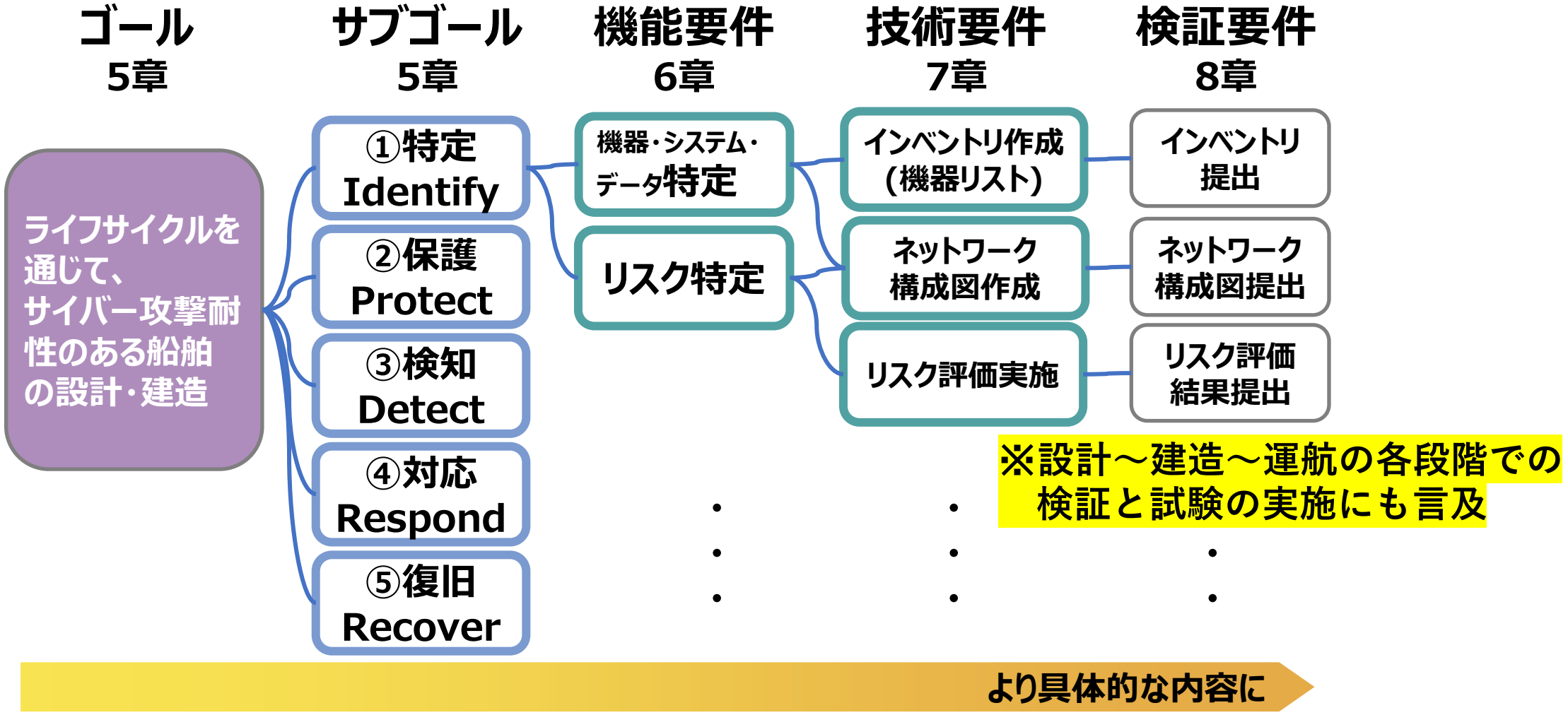
Appendix A contains a detailed list of standards which this Recommendation makes

Page 2 of 57 IACS Rec. 2020/Corr.1 2020

Recommendation on Cyber Resilience , IACS
Apr.2020 (Corr.1 July 2020) ,57 Pages
ダウンロード：http://www.iacs.org.uk/download/10714

4) 船舶建造におけるサイバーレジリエンス向上

IACS Recommendation on Cyber Resilienceの構成



3．業界内での議論と対応

ご参考

舶用機器や船舶のサイバーセキュリティに関する海外船級の主な認証取得状況

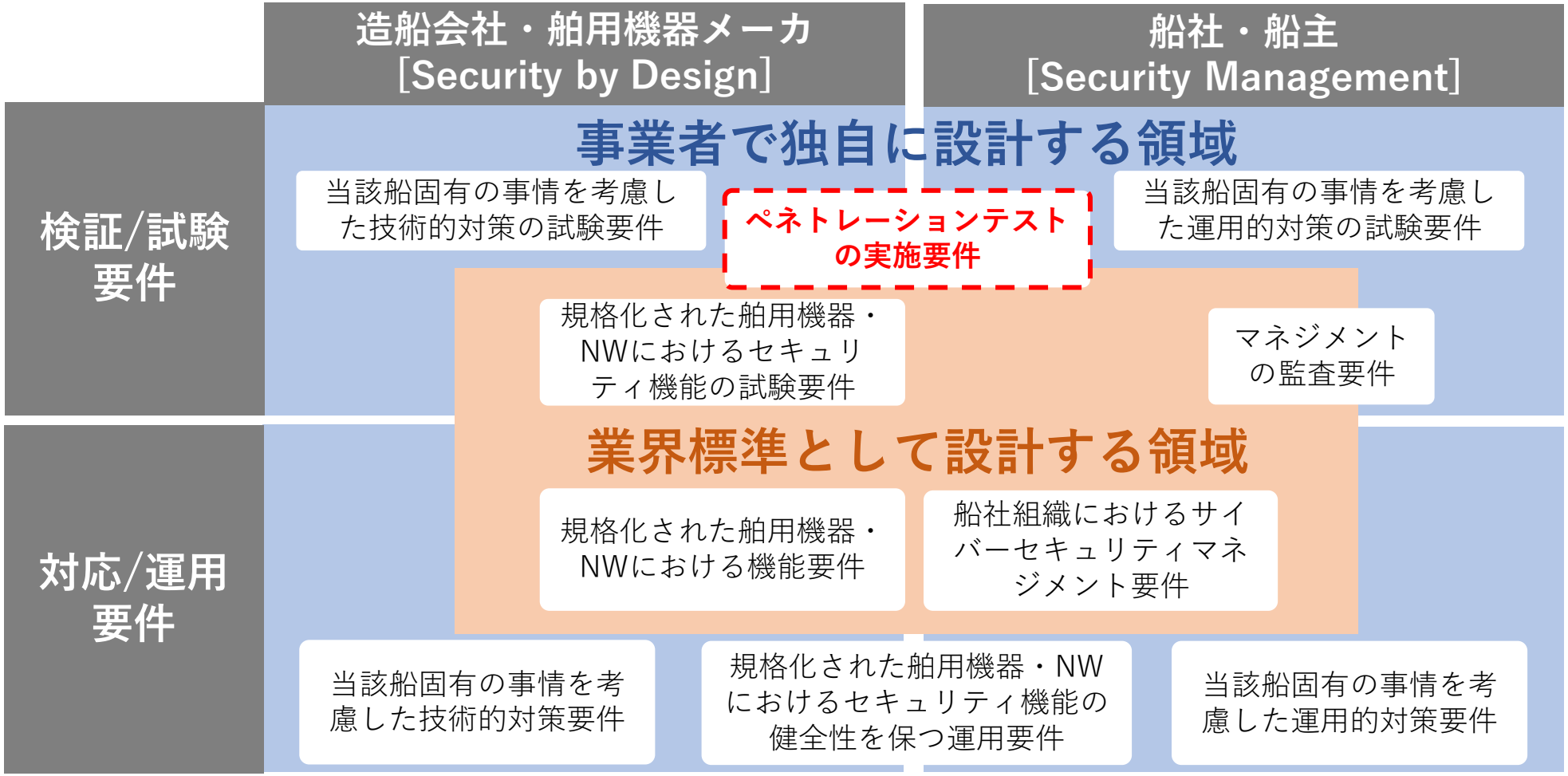
2020年８月弊社調べ

日付	船級	取得メーカ(国名)	認証内容
2017年11月	DNV-GL	Kongsberg Maritime（ノルウェー）	同社のVPMS　K-IMSが型式認証DNVGL-CP-0231を取得
2018年1月	LR	Nantong COSCO KHI Ship Engineering （中国）	同社のコンテナ船が「Cyber AL3 SECURE PERFORM (Energy Management System)」を取得
2018年11月	ABS	現代重工業（韓国）	同社及び同社のVLCC船がCS-Ready Notationを取得
2019年2月	KRS	Songa Shipmanagement（英国）	同社がサイバーリスクマネジメントのCertificationを取得
2019年2月	DNV-GL	Naval Dome（イスラエル）	同社のエンドポイント防御システムが型式認証DNVGL-CP-0231のSL4（最高レベル）を取得
2019年6月	KRS	現代重工業（韓国）	同社のHyundai-ISCSがサイバーセキュリティの型式認証を取得
2019年7月	LR	大宇造船海洋（韓国）	同社のECDIS等を含む艦隊監視システムが「Digital AL3 SAFE SECURITY」のAiPを取得
2019年8月	LR	現代重工業（韓国）	同社のネットワークセキュリティデジタルコンポーネントが型式認証を取得。
2019年11月	DNV-GL	現代重工業（韓国）	同社が建造中のLPG船がCyber Secure (Advanced) のAiPを取得
2019年11月	DNV-GL	サムスン重工業（韓国）	同社のSVESSEL®がCyber Secure(Advanced+）のAiPを取得
2019年12月	LR	Wärtsilä（フィンランド）	同社の統合システムネットワークが「SAFE AL2」のAiPを取得
2020年 5月	BV	France LNG Shipping SAS (**NYK**とGeogas LNG SASの共同船舶保有会社) (フランス)	現代三湖重工業（韓国）にて建造した、同社の保有のLNG運搬船が、BV SYS-COM Notationを取得**（LNG船では世界初の取得）**

目次

1) ペネトレーションテスト検証の位置づけ

ペネトレーションテストの実施要件は、サイバー対策の検証において、
業界標準で設計する領域と、**事業者独自で設計する領域**にまたがる。



1) ペネトレーションテスト検証の位置づけ

業界ガイドラインでは、現時点ではペネトレーションテストを**義務付けてはいない**が、
試験実施の**推奨**や、**高いレベルの船級認証では実施が求められる**場合もある。

組織名	IACS 国際船級連合	ABS （アメリカ 船級）	DNV-GL （ノルウェー 船級）	BV （フランス 船級）
文書名	IACS Recommendation No. 166 “Recommendation on Cyber Resilience”*	CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES ABS CyberSafety™ VOLUME 2**	DNVGL-RU-SHIP “RULES FOR CLASSIFICATION Part 6 Additional class notations Chapter 5 Equipment and design features”***	NR 659 DT R00 “Rules on Cyber Security for the Classification of Marine Units”****
Notation名	(N/A)	CS-Ready, CS1, CS2, CS3	Cyber secure	CYBER MANAGED, CYBER SECURE
ペネトレーションテストの扱い	●**設計段階および、船舶建造完了直前の機能検証する手段として、“試験”を実施すべきと言及**	● 最も厳しいNotationである”CS3”の要件として、**運航後の定期的なペネトレーションテストの実施を規定**	●「要求通りの作りとなっているか」を検証する統合試験の実施を規定 ● ペネトレーションテストは、**検証の手法として例示**	● 自律機能を有する船舶を対象としたNotationである”CYBER SECURE”の要件として、建造時の**ペネトレーションテストの実施を規定**

* http://www.iacs.org.uk/download/10714
** https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety-V2-Cybersecurity-Guide-June18.pdf
*** https://rules.dnvgl.com/docs/pdf/DNVGL/RU-SHIP/2020-07/DNVGL-RU-SHIP-Pt6Ch5.pdf
**** http://erules.veristar.com/dy/data/bv/pdf/659-NR_2018-12.pdf

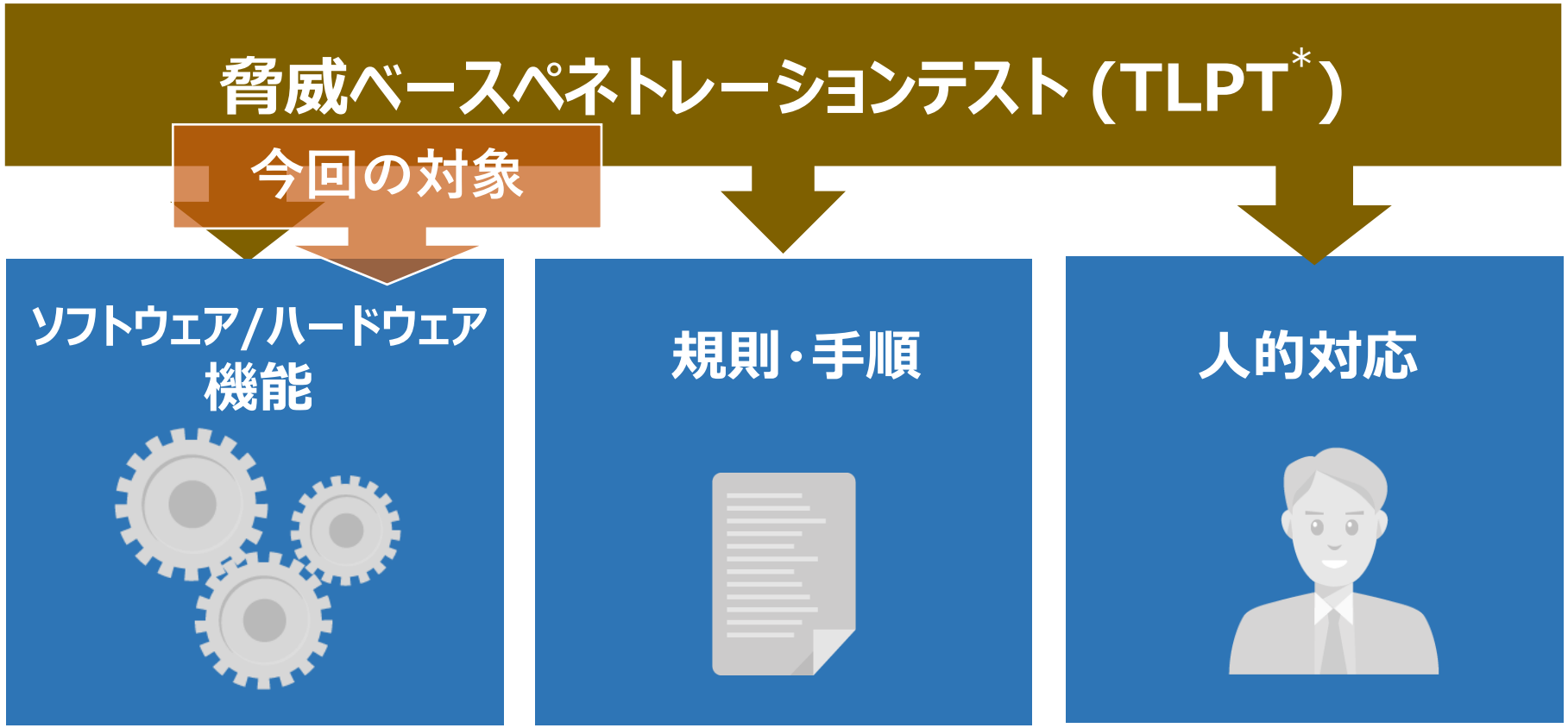
2) 船舶ペネトレーションテスト 検証PJ (2019年10月～2020年7月)

海運業界の各プレイヤーが連携し、サイバーセキュリティ専門家の協力を仰ぎながら、
ペネトレーションテストの**知見の獲得**と、検証手段としての**各種課題の抽出**が目的

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	

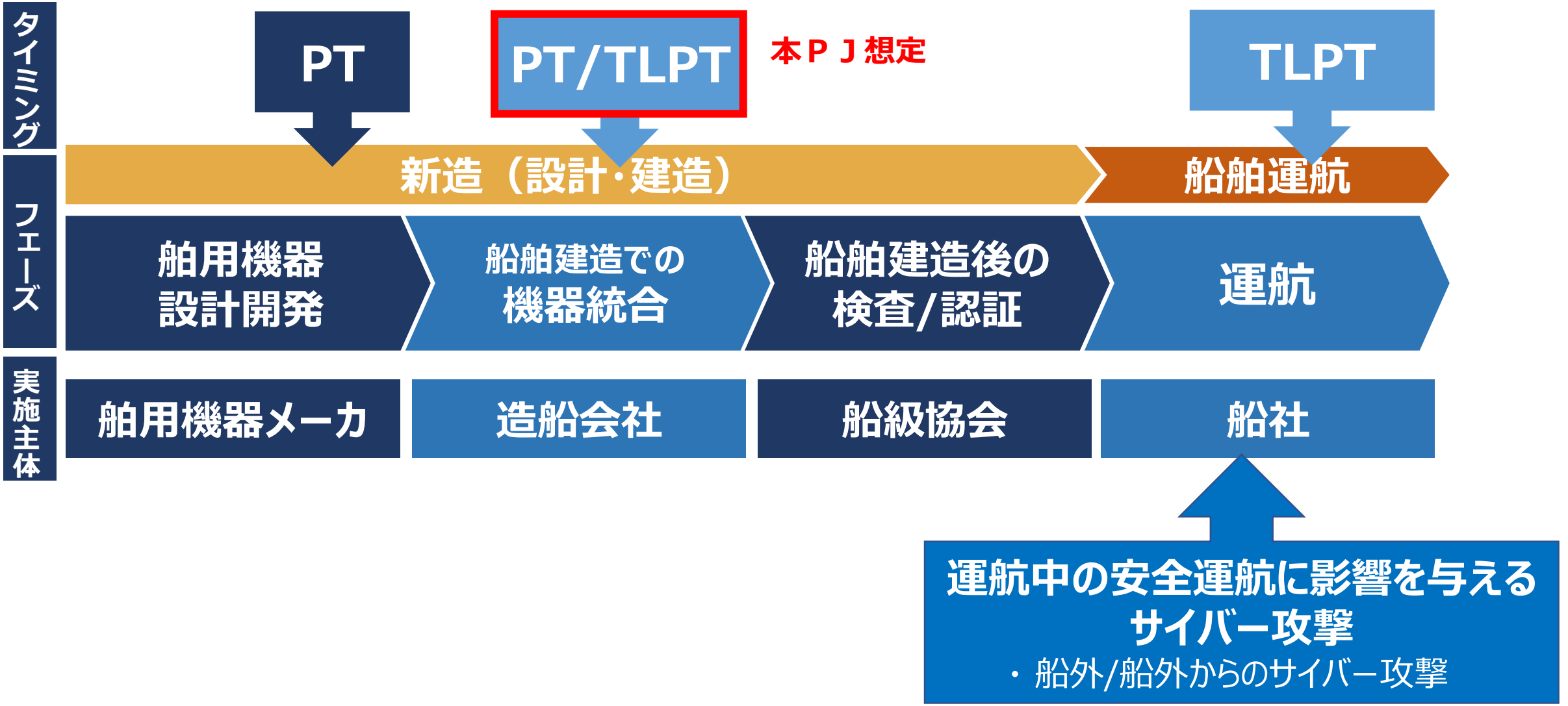
3) ペネトレーションテストのタイミングと実施主体

安全運航に大きな影響を与えるサイバーインシデントのシナリオを定義し、当該脅威の顕在化を目的とした。今回は**ソフト・ハードウェア機能に限定したTLPT**検証を実施



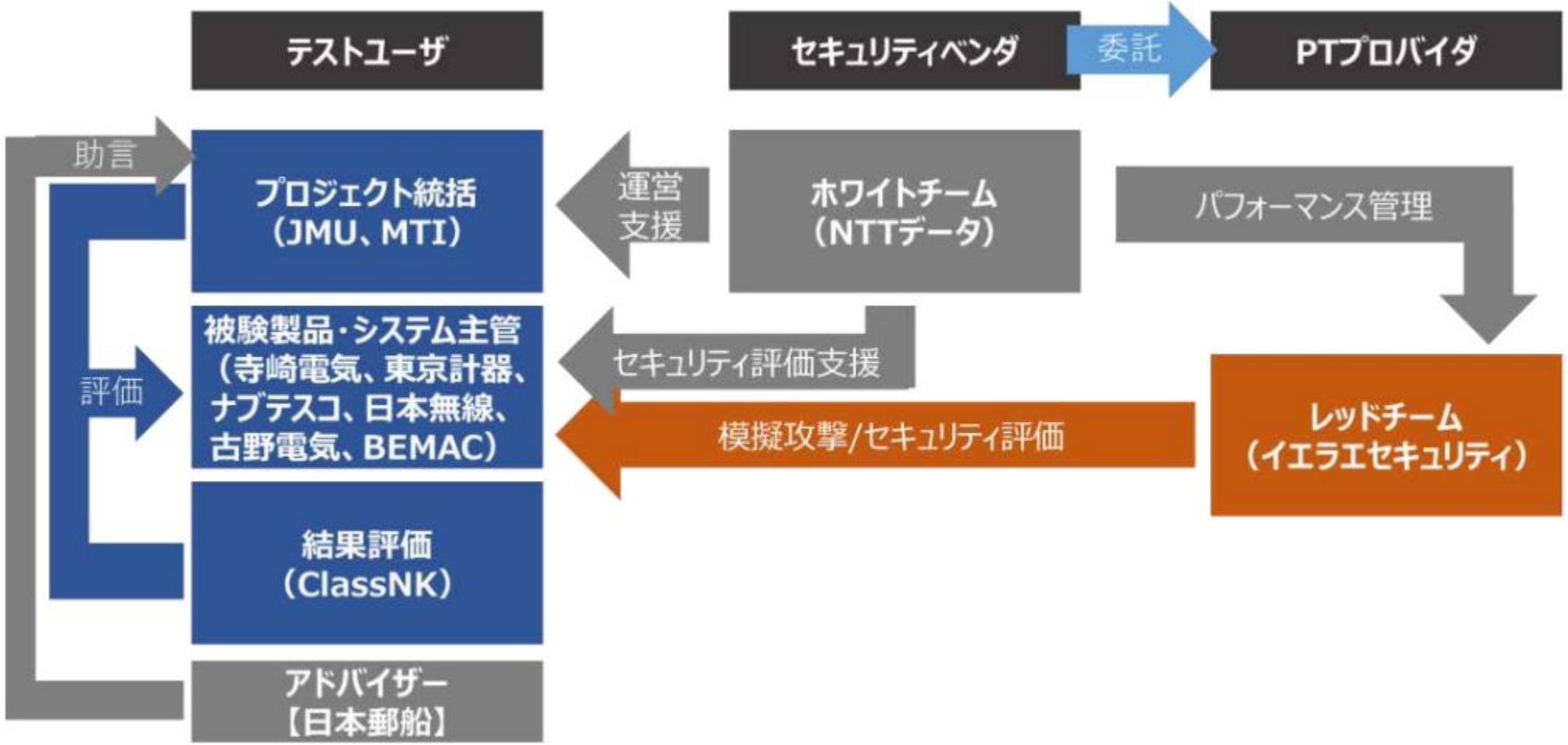
＊ TLPT ＝ Threat Led Penetration Test

3) ペネトレーションテストのタイミングと実施主体



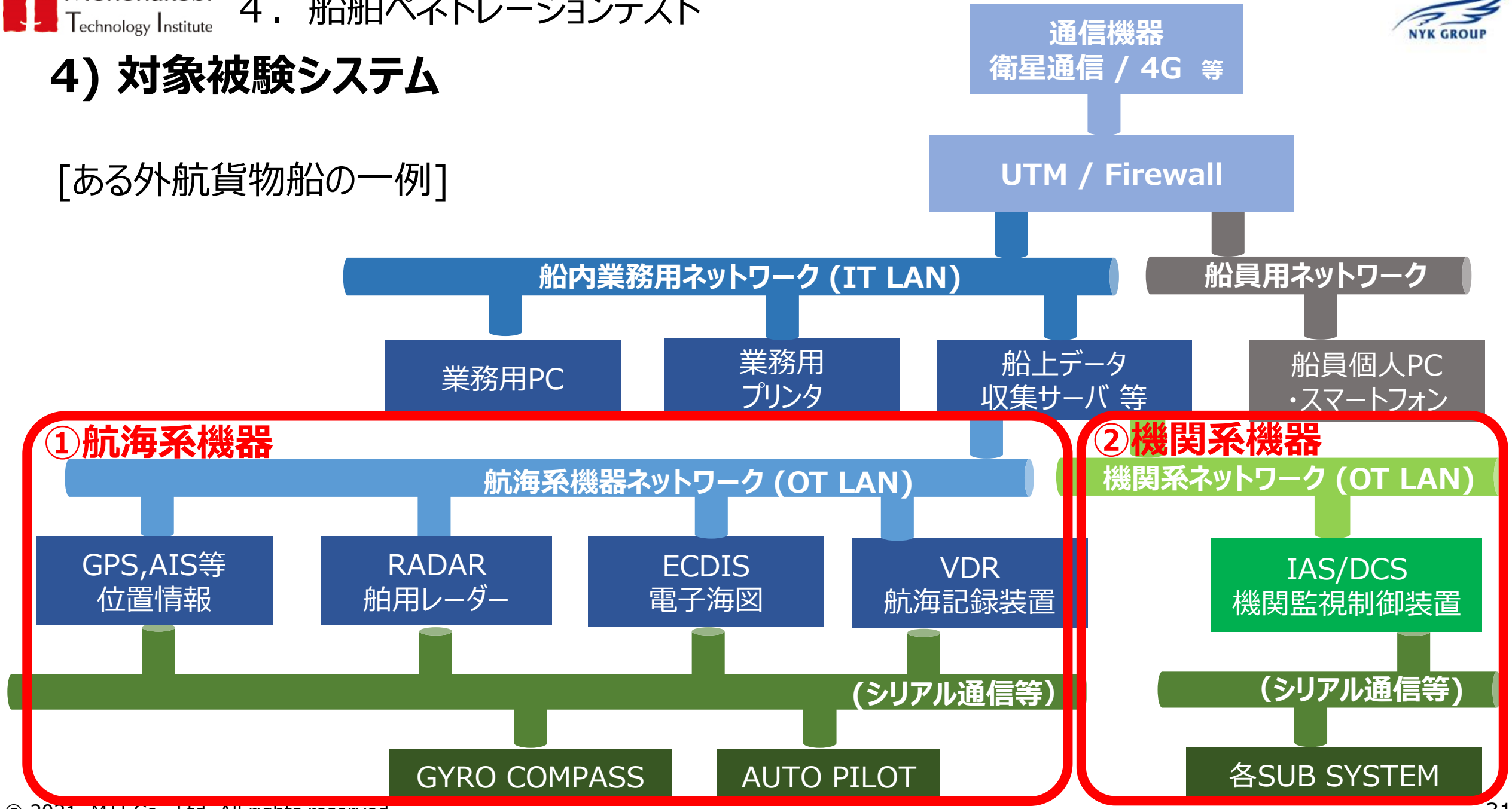
3) ペネトレーションテストのタイミングと実施主体

造船会社によるPT/TLPTを想定し、インシデントシナリオ作成には**船会社**、
検証結果の評価および今後の課題抽出には**船級協会**とも協力して実施。

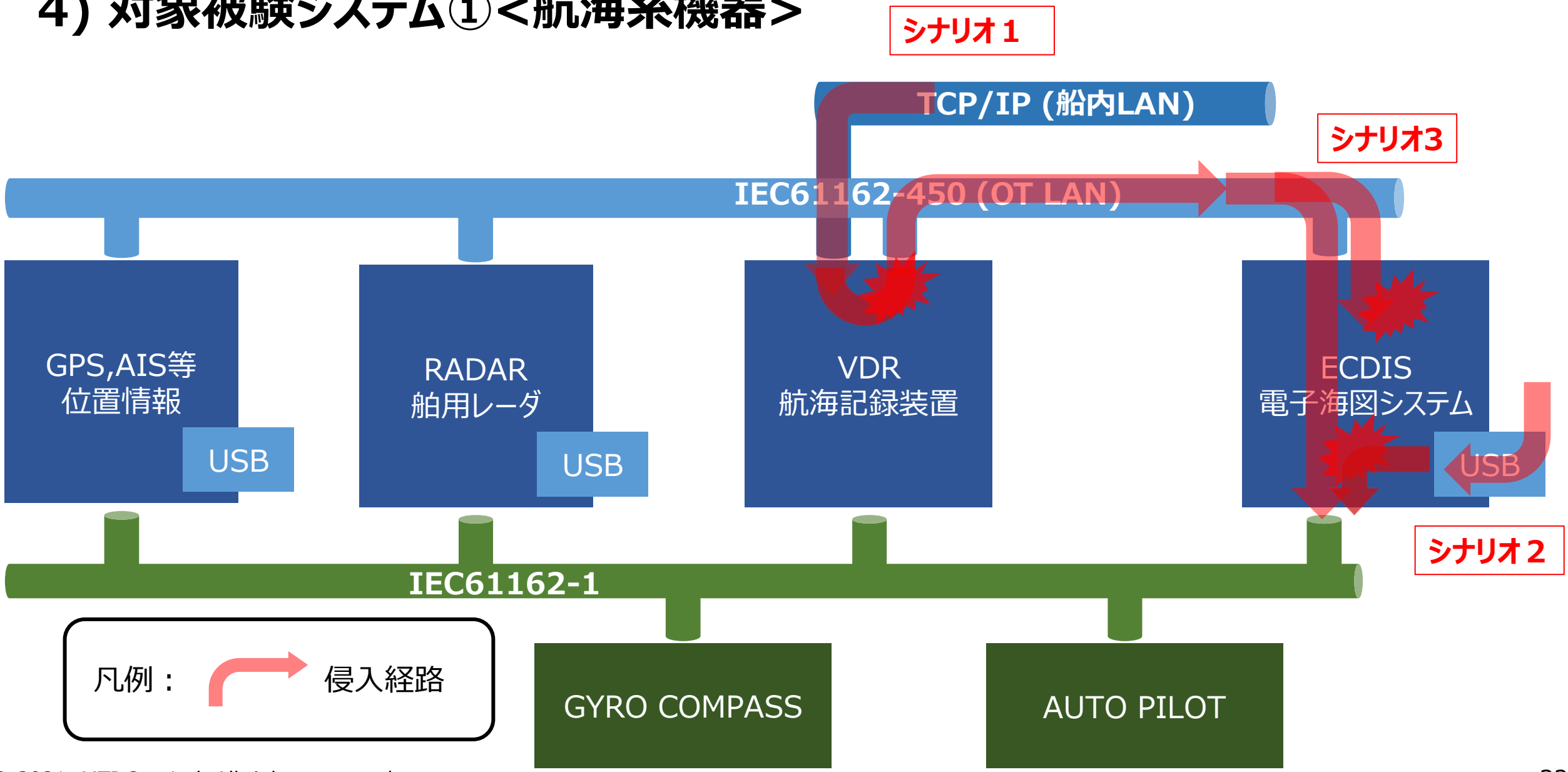


4) 対象被験システム

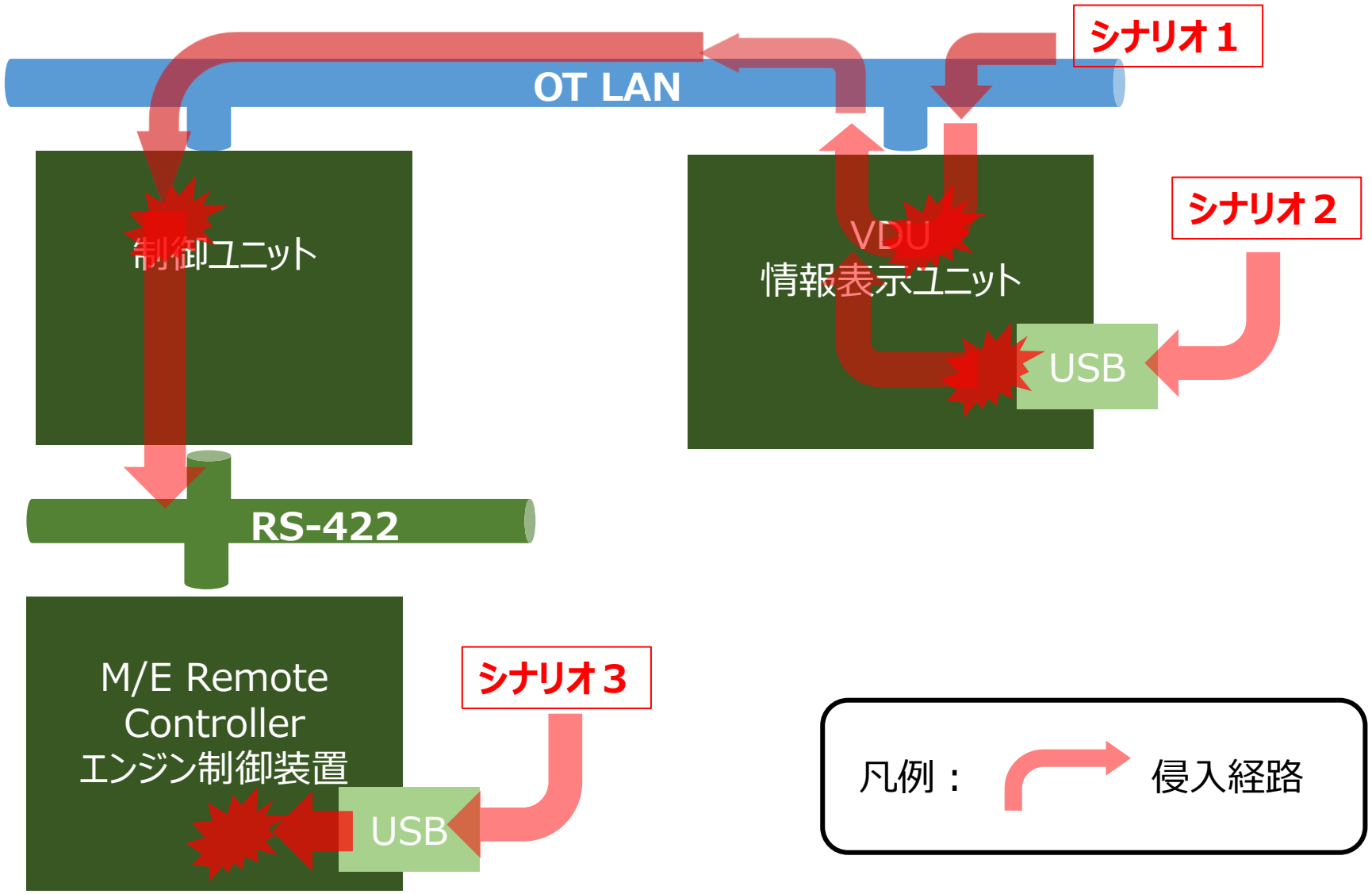
[ある外航貨物船の一例]



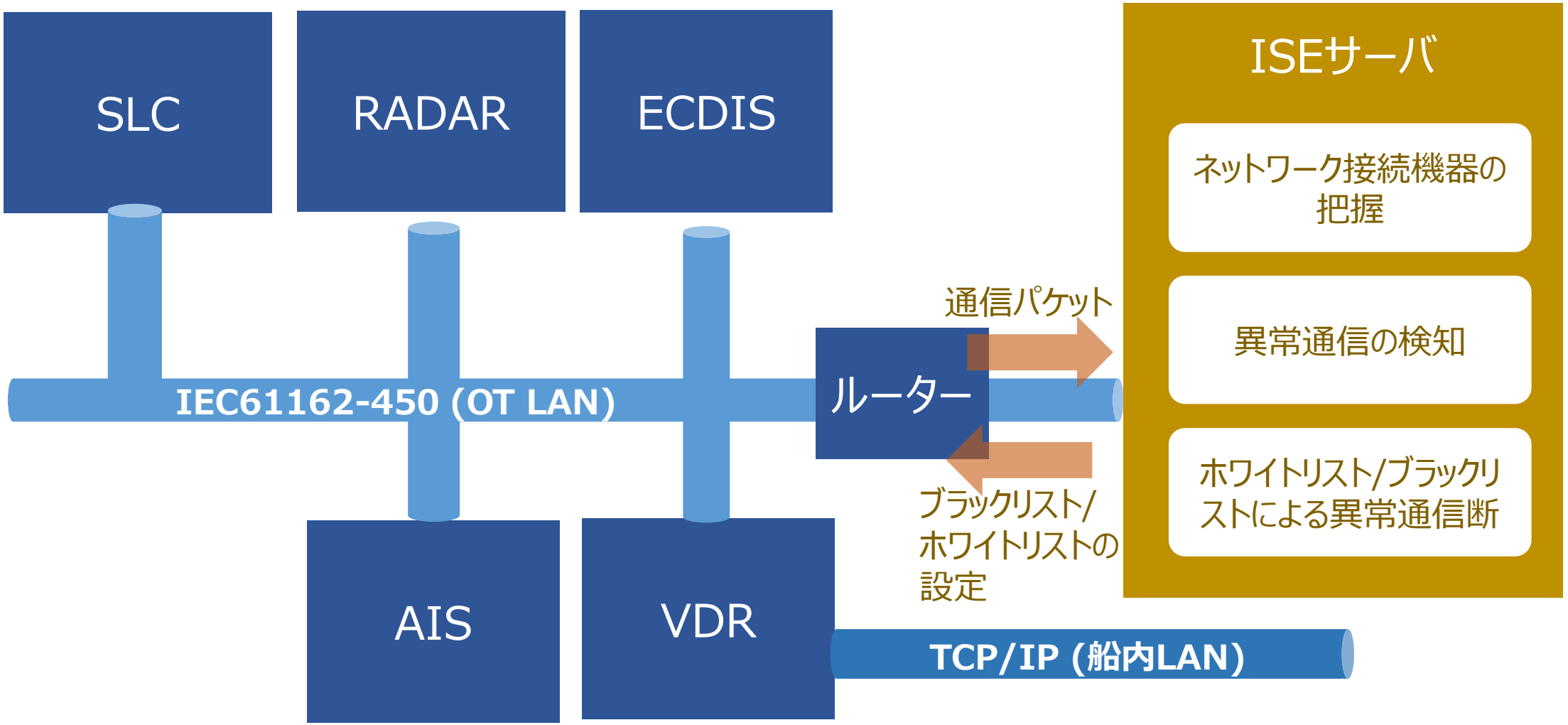
4) 対象被験システム①<航海系機器>



4) 対象被験システム②＜機関・エンジン系機器＞



5) 対策技術の検証 <IoTセキュリティオーケストレーションエンジン(ISE)>



*ISE：NTTセキュアプラットフォーム研究所により開発されたサイバー攻撃検知技術

6) テスト結果① <対策されていた例>

大分類	小分類	レッドチーム攻撃に対して対策済みであった項目
REDSセキュリティ		キーボード操作を模擬できるBadUSBを用いて侵入を試みたが、BadUSBからの文字列入力はアプリケーションに入力されたため、**任意コマンドの実行には失敗**した。
ソフトウェアメンテンナンス		OS/インターフェースに**既知の脆弱性が存在しなかった**。
ユーザ認証/認可	認証実施	ある航海機器が提供するサービスには**すべて認証が求められており**、認証情報についても容易に入手できないよう設定・管理されていた。
	権限設定	提供するサービスへアクセスするアカウントに与えられる**権限を限ることで**、**当該アカウントで実施できる操作を限定**している。
公開設定	適切なポート・サービス公開	必要最低限のサービスのみを提供しており、**不要なサービスは提供していない**。このことにより、レッドチームのエントリポイントが限定された。
	適切なファイル公開	レッドチームは、当該機器から電文を発出する操作を実現するための情報収集を当該機器内のファイルを閲覧することによって行うが、**公開サービスのアカウントで閲覧できるファイルは限定されている**。

6) テスト結果② <対策が必要だった例>

大分類	小分類	明らかになった検討事項
REDSセキュリティ		USBポートから**特殊キー操作が有効**
ソフトウェアメンテンナンス		Windowsベースの機器、**既知のWindowsの脆弱性が存在**
ユーザ認証/認可	認証の不備	● 同一LAN内であれば重要なデータが存在する領域に**匿名アクセスが可能** ● **認証なしで**重要な機能へアクセス可能 ● Windowsの**管理者アカウントにパスワードが設定されておらず**、ネットワーク経由でファイル読み書き可能
	権限設定の不備	機器管理画面において、Guestアカウントで**Administratorアカウント権限と同様の操作が可能**
	貧弱なID/パスワード	**デフォルトのパスワード**、もしくは容易に推測可能なパスワードを設定
公開設定	不要なポート/サービス公開	公開**不要なポート/サービスを公開**
	不要なファイル公開	● 公開不要な機器上のファイルが**外部から閲覧可能** ● ディレクトリリスティング機能が有効になっており**ファイル一覧情報を取得可能** ● 企業のウェブサイト上に，公開を想定していない**機器関連情報のファイルを公開**

7) ペネトレーションテストPJのまとめ

■結果と成果

✓船舶ペネトレーションテスト実施に必要な**連携体制・手順の知見を獲得**

✓機器の動作停止、データ改ざん、不正データ偽装送信などが可能となったケースが小数例ではあるが存在することが判明。それぞれの**対策案が確認された**

✓ペネトレーションテストの、**船舶建造の検証・試験における有用性を確認**

➡**「実施成果報告書」として、WEB一般公開**

https://www.nyk.com/news/2020/20200720_01.html

■今後求められるアクション

✓テスト実施の**タイミング・主体者・方法**について業界内での議論 (When/Who/How)

①機器開発段階：舶用機器メーカによる機器へのPT

②船舶建造段階：造船会社によるPTおよびTLPT

③就航後：船会社・船主による定期的なTLPT実施による健全性評価

➡**海運ビジネスとしてのコスト・メリットも考慮して業界内での合意形成も必要**

目次

海運における船舶サイバーセキュリティ対策　まとめ

- ✓ 舶用機器や、船陸通信の高度化に伴い、**船舶サイバーセキュリティ対応（特にOT機器）**が世界的に急務となっている。
- ✓ **2021年1月以降、安全運航のための”船舶サイバーリスク対策”が必須**となり、船会社・船主・造船会社では、それぞれ対応を進めているが、各プレーヤが効果的に**連携して、対策・対応にあたる体制作り**が重要。
- ✓ 業界内でガイドラインやルールは作成されつつあるが、**検証する仕組みや体制は、まだ議論の途中**である。
- ✓ 今後、**検証手法としてペネトレーションテストは有用**であるものの、実施タイミングや主体社については、**海運ビジネスの特性も考慮した議論が必要**

ご清聴ありがとうございました。