船舶サイバーセキュリティ対策

2020年11月27日

株式会社MTI　船舶物流技術グループ
柴田　隼吾

目次

目次

1．はじめに

- ✓ 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**
- ✓ 一方で、機器高度化や常時接続に伴い、外部からのマルウェア感染、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**
- ✓ これら背景のもと、2017年6月の国際海事機関（IMO）第98回海上安全委員会（MSC98）において、船主・運航者はサイバーリスク管理に関して、ISMコードに基づき、**安全管理システム(SMS)に記載***することを**“推奨”**するガイドラインが採択される。

※2021年１月以降の最初の年次検査までに

“Recomandatory”

1．はじめに

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＝操船乗っ取りや運航不能を防止するために、船の各ファンクションを正常に保つこと。

■その他にも守るべき対象はさまざま：

例） IT機器や、そこに含まれる情報：**損傷、改変、悪用**からの保護

船陸間通信：**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とは：**

・**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**

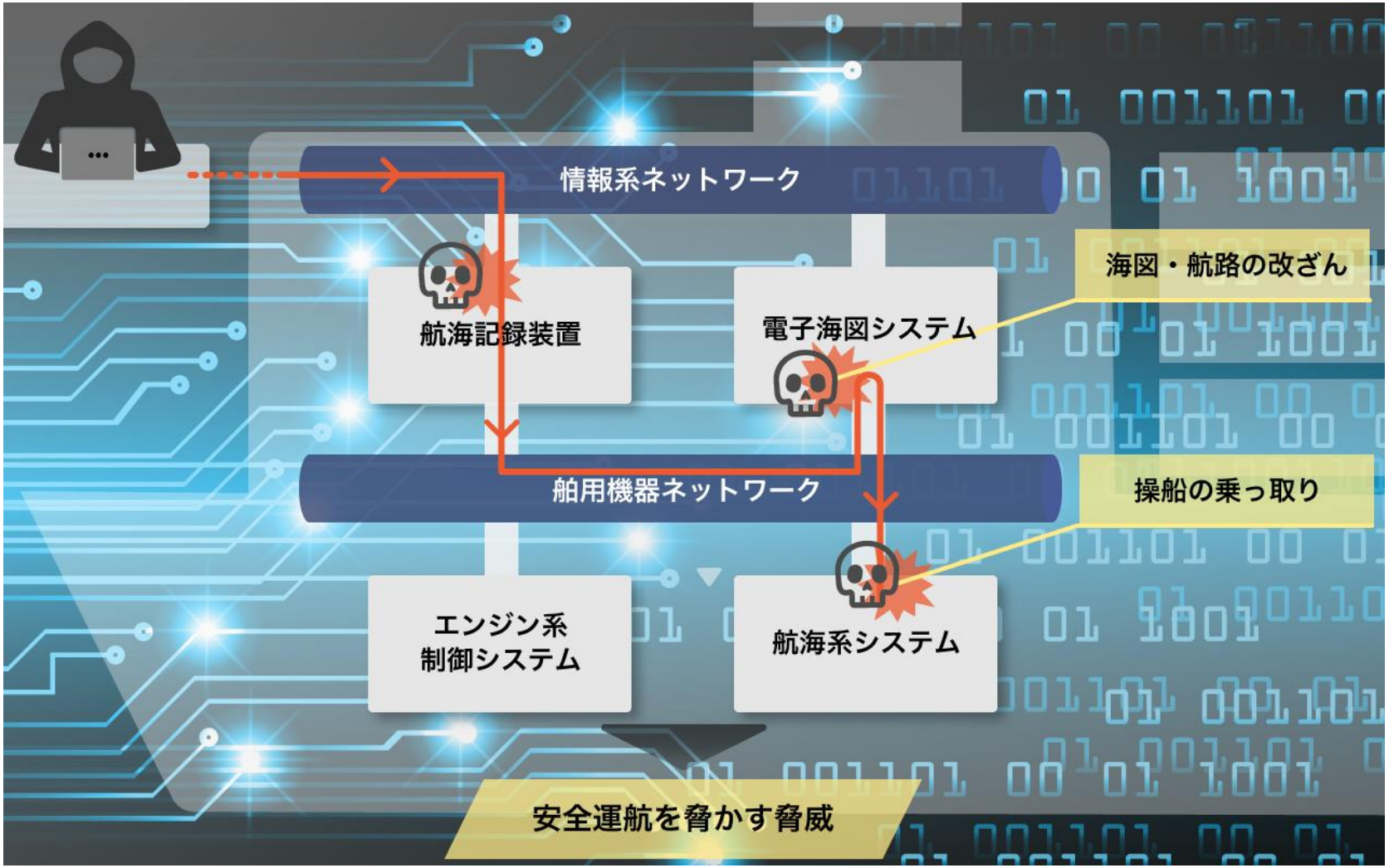
攻撃例：マルウェア、ランサムウェア、GPS信号なりすまし

1．はじめに

	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、Biz-PC、プリンタ および情報ネットワーク　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、取引情報保護 データ暗号化	・データ漏洩の影響度は低い 例）機器設定値 運航状態データ
完全性 [**I**ntegrity]	・**データや情報の改ざん防止** ・情報整合性の保持が重要	・**物理制御の正常動作が重要** ・**物理的な安全性が最優先** ・リスクの影響が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	・**制御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 ・緊急対応ができることが重要

１．はじめに

船舶OT機器への攻撃イメージ

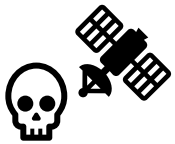


海事分野でのOT攻撃インシデント事例
①ハッキングによる操船乗取り

- ✓2017年2月キプロスからジブチに向かう、ある8,250TEUのコンテナ船が**約10時間にわたり操船システムを乗っ取られる。**
- ✓“**突然、船長が操縦できなくなった。ナビゲーション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。
- ✓**外部から加わったIT の専門家と連携し**何時間も対応し、なんとか攻撃をブロックすることが出来た。
- ✓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もあるが、**原因はいまだ不明。**

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

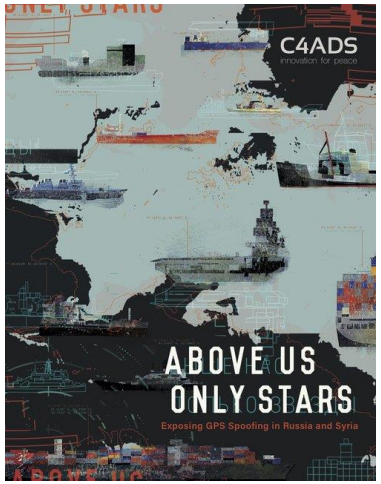
海事分野でのOT攻撃インシデント事例
②GPS信号の改ざん(スプーフィング)

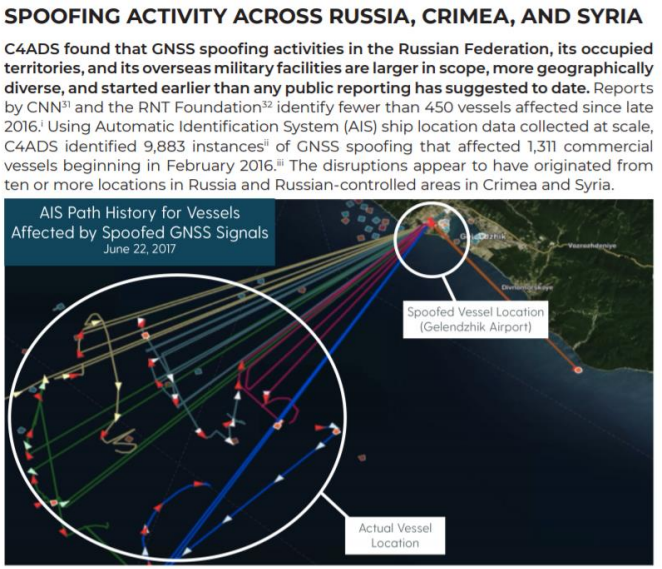


✓黒海付近で、数年間で**1万件以上の**GPS位置情報の改ざん発生

✓**1000隻以上の商船の航行に影響**

✓2019年3月 米国シンクタンク(C4ADS)は、これは**ロシア軍によるGPS信号なりすまし行為が原因**であると報告





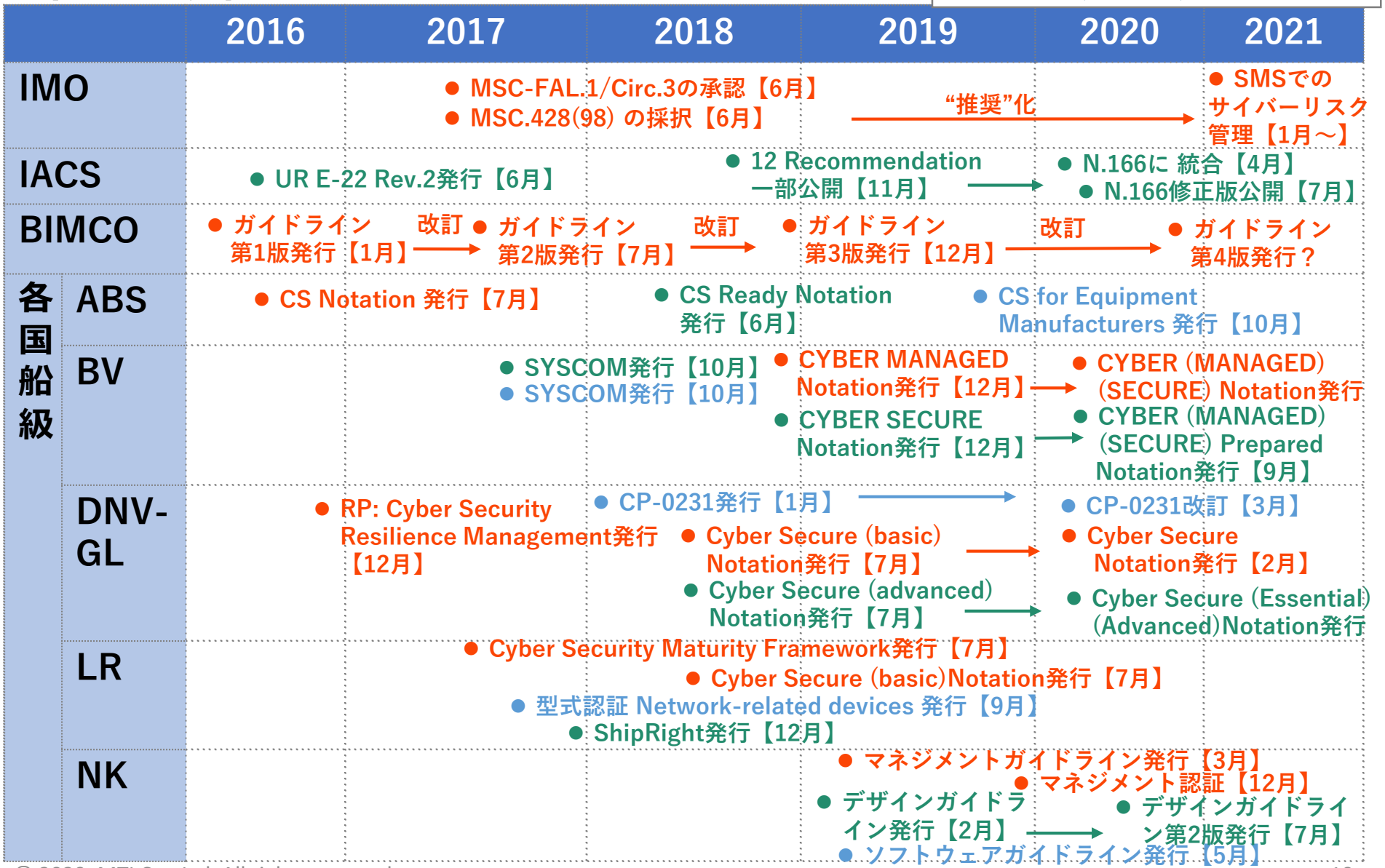
出典：Above US ONLY STARS, The Center for Advanced Defense Studies
米国高等国防研究センター（C4ADS）, 2019年3月発行

目次

2．各ガイドライン・認証①

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

これまでの流れ



2．各ガイドライン・認証②

それぞれを整理すると、

凡例：船級・各国船級　船技協が実施　個社が実施

		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	造船所	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、各機器メーカが対応実施	Cyber-Resilient shipガイドライン等に基づき、造船所・船社が対応実施	CSMSテンプレートに基づき、各船社がSMSでの対応を実施 (2021年1月～)
	検証(Check)	船舶機器・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

*船技協 ：(一財)日本船舶技術研究協会

目次

3．船舶運航におけるリスク管理

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

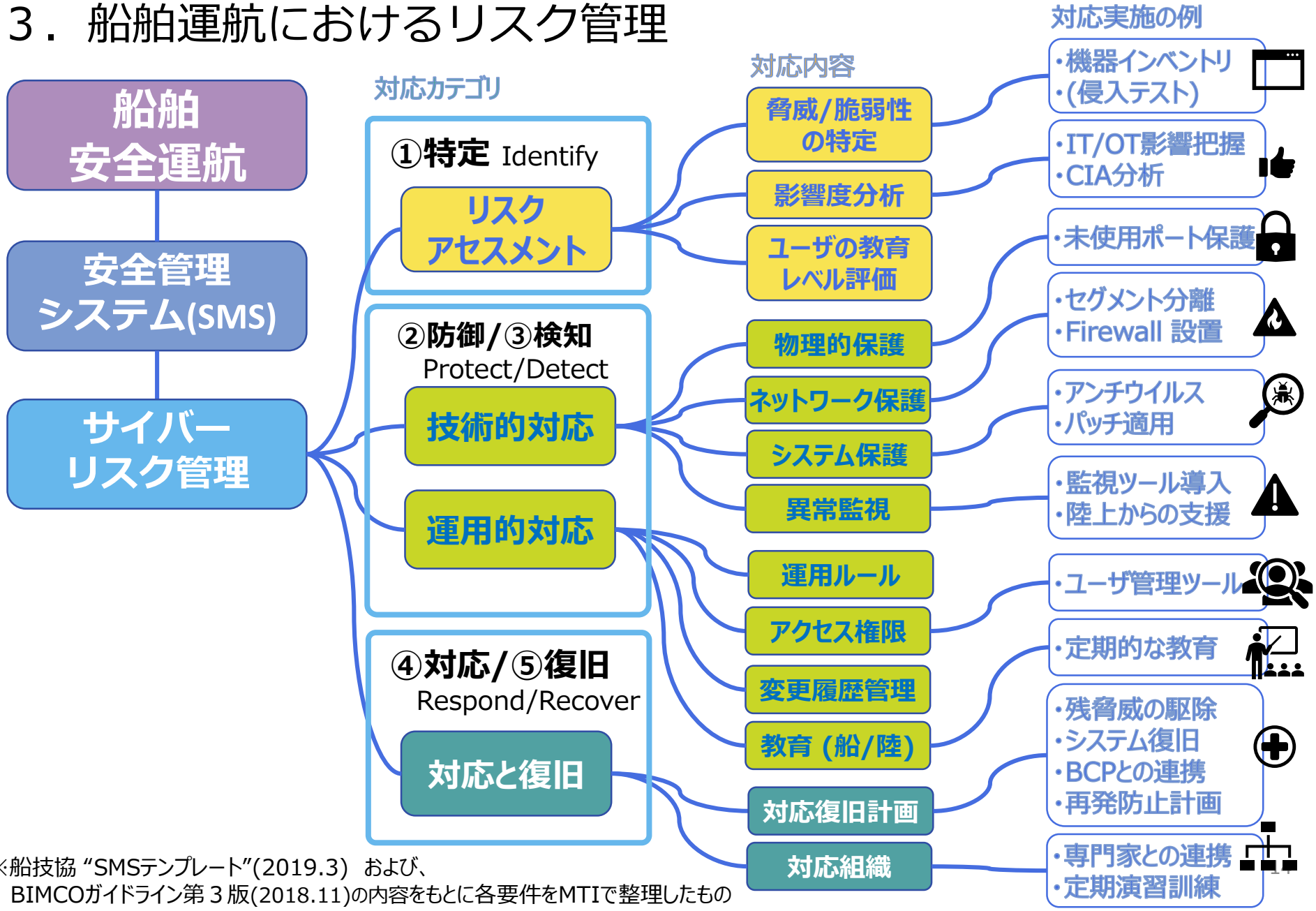
サイバーリスク管理アプローチ：

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．船舶運航におけるリスク管理

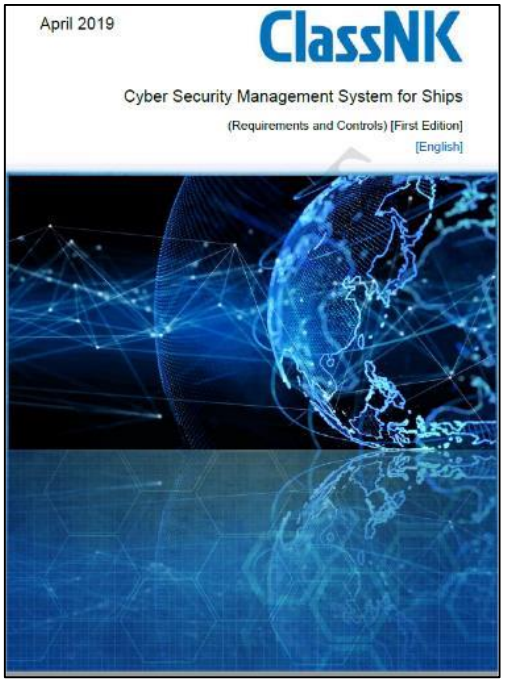


※船技協 “SMSテンプレート”(2019.3) および、
BIMCOガイドライン第３版(2018.11)の内容をもとに各要件をMTIで整理したもの

NYK運航船における、サイバーリスク管理認証取得

LNG船 PACIFIC MIMOSA
ClassNK サイバーマネジメント認証取得

- ✓ **2019年12月**
  日本海事協会による初めてのCSMS認証
- ✓ **運航船のサイバーセキュリティ管理手順に関する任意認証**

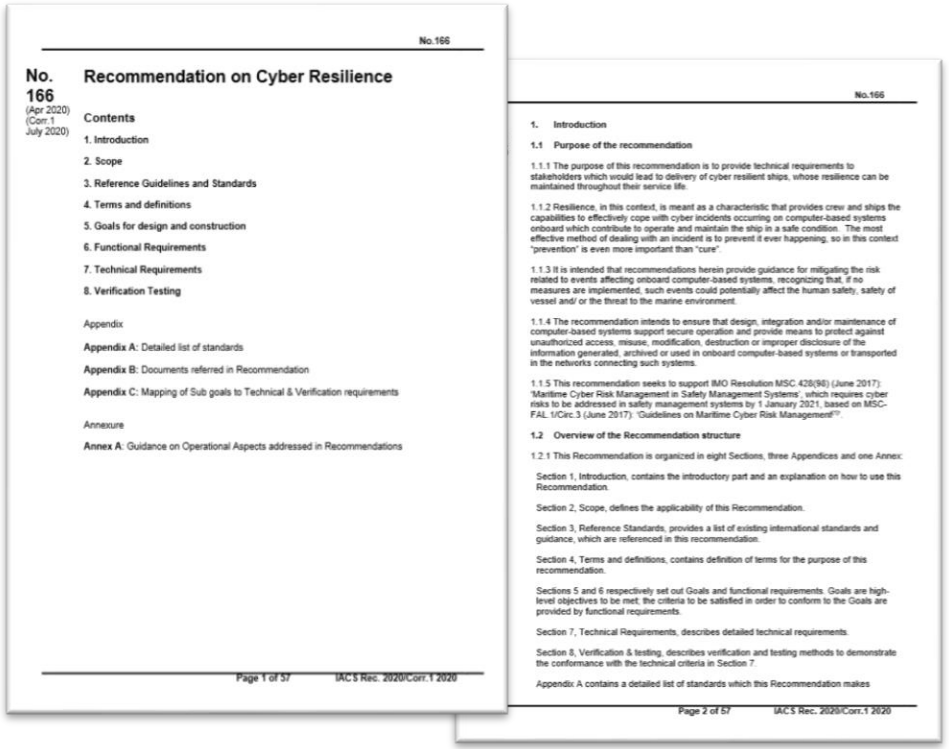


日本郵船プレスリリース：https://www.nyk.com/news/2019/20191216_01.html

目次

4．船舶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)



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

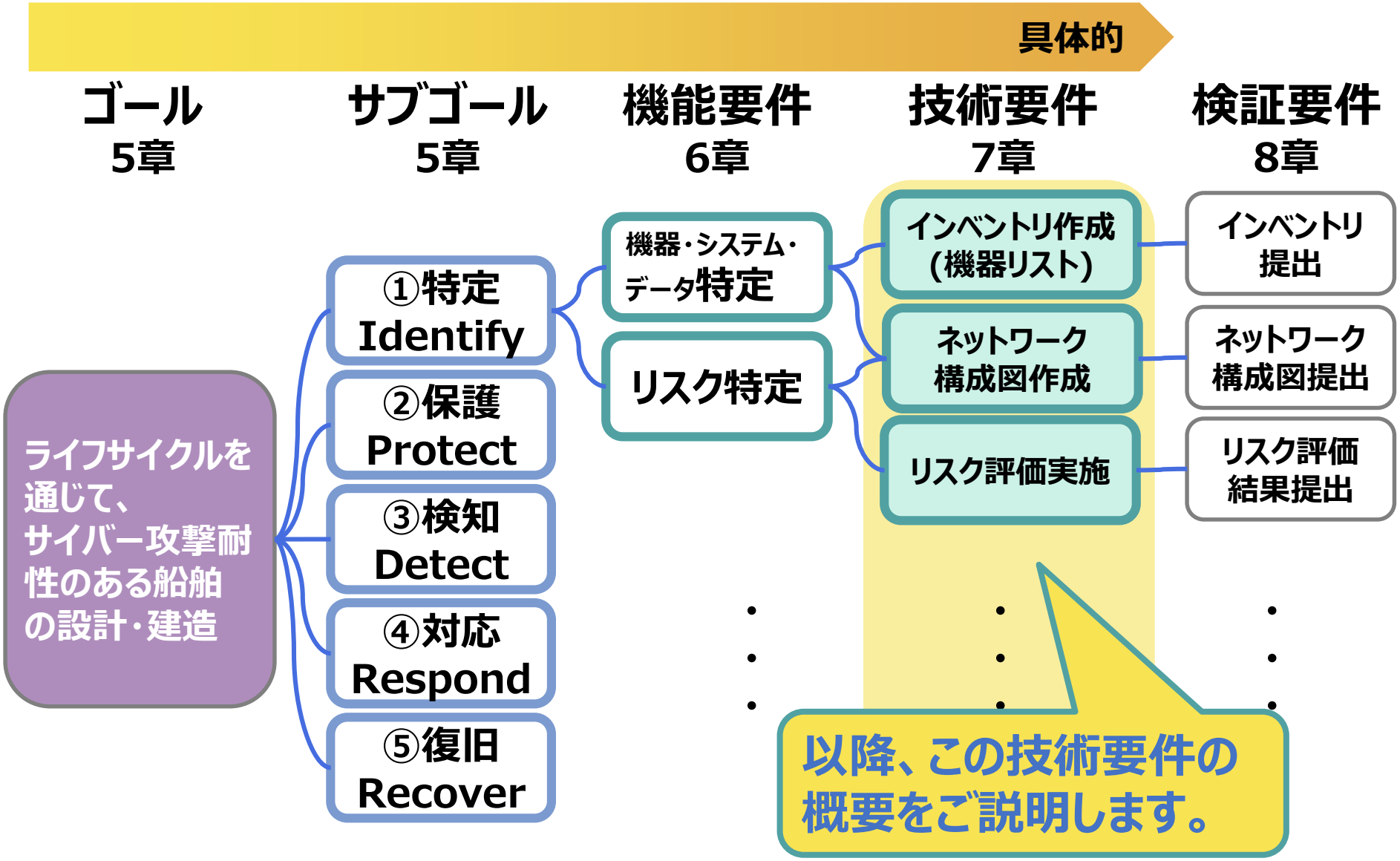
Page 2 of 57 IACS Rec. 2020/Corr.1 2020

目次

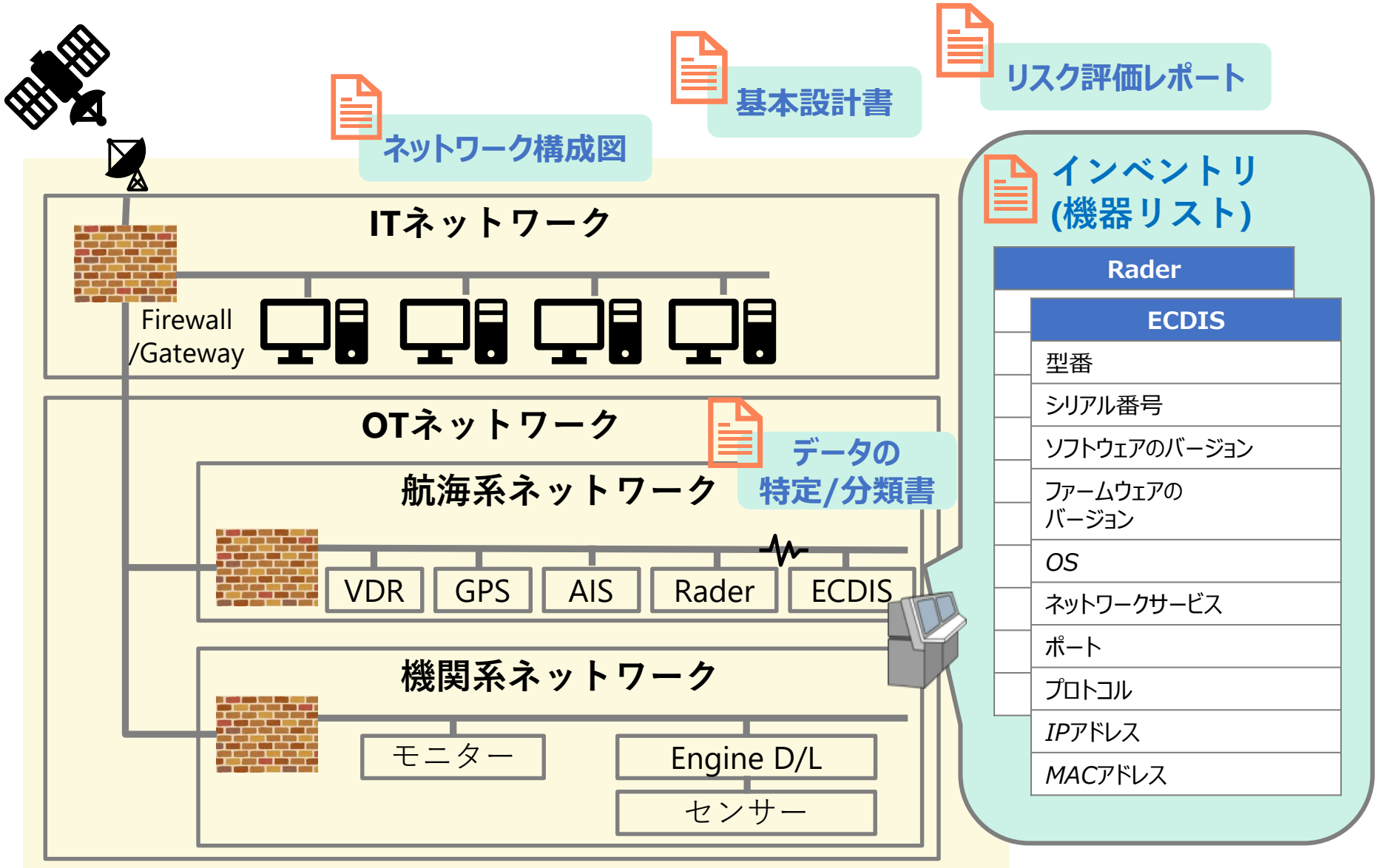
Recommendation on Cyber Resilience , IACS Apr.2020(Corr.1 July 2020) ,57 Pages

http://www.iacs.org.uk/download/10714

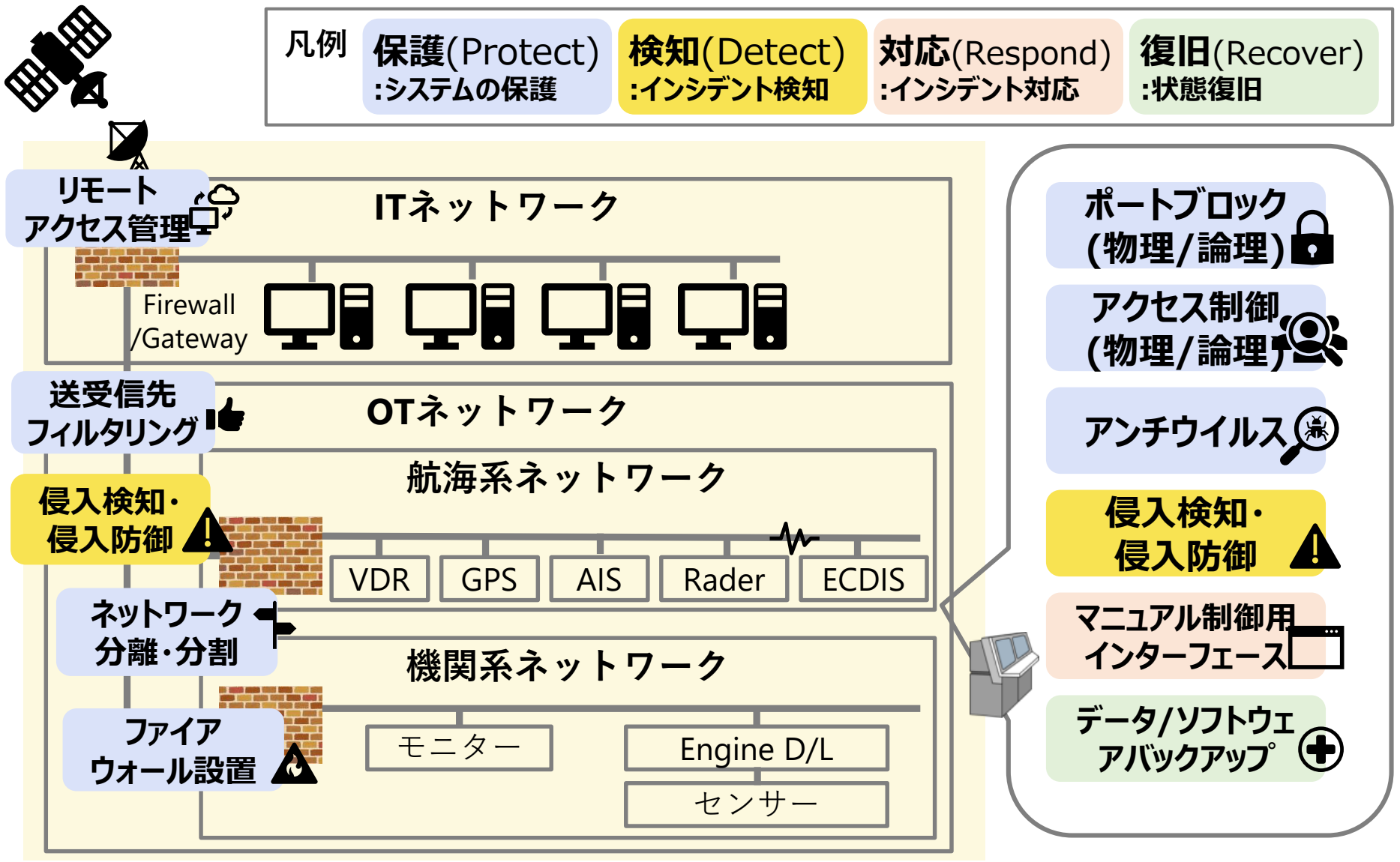
IACS Recommendation on Cyber Resilienceの構成



①特定 (Identify) の技術要件



②保護(Protect)～復旧(Recover) の技術要件



③それぞれの役割とフロー

凡例：
船級の確認・認証

船舶のフロー

文書のフロー

荷主

船主・運航者

造船所

舶用機器メーカ

サイバーセキュリティ要求の提示

サイバーセキュリティ要求の提示

運航時のサイバーリスク管理

船舶引き渡し

文書引き渡し

・要求に基づき新造設計

・設計に基づきインテグレート
・試験の実施

・収集した文書の管理
・船舶全体に係る文書作成

要求に基づいた機器・システム調達

要求に基づいた機器・システム納入

機器・システムに関する文書の提供

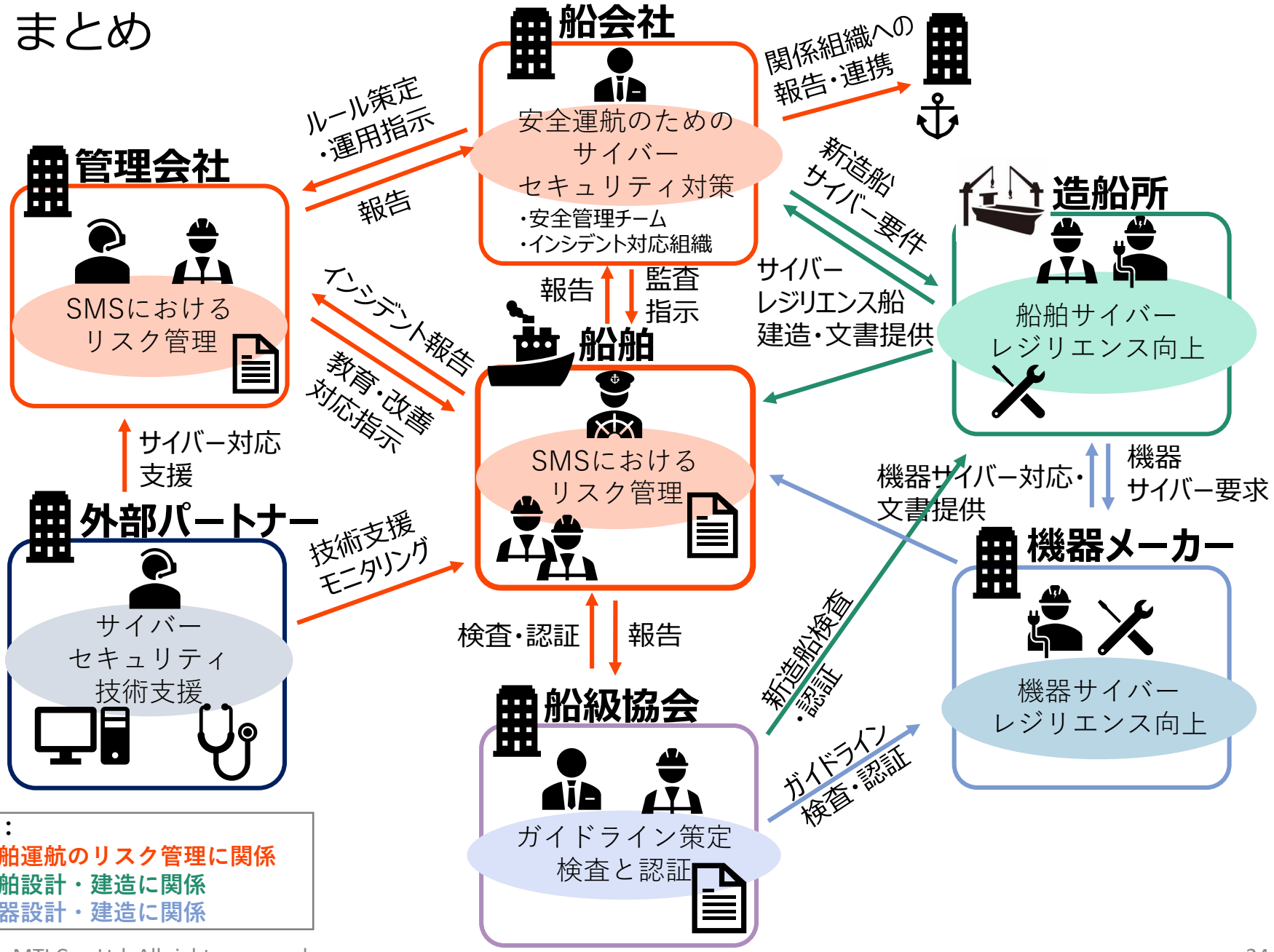
ご参考

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

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）**

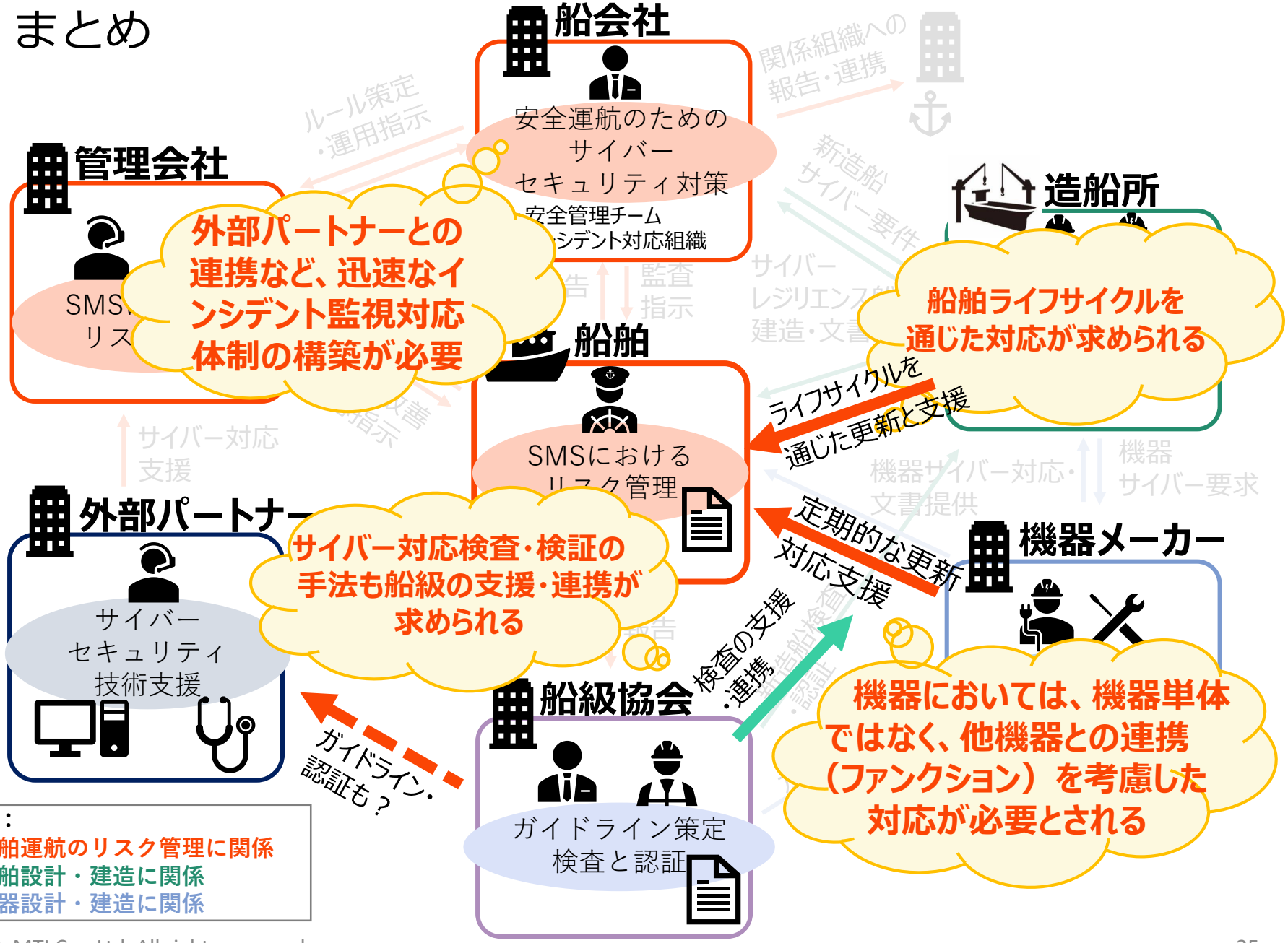
目次

5．まとめ



凡例：
- ➡船舶運航のリスク管理に関係
- ➡船舶設計・建造に関係
- ➡機器設計・建造に関係

5．まとめ



凡例：
- ➡船舶運航のリスク管理に関係
- ➡船舶設計・建造に関係
- ➡機器設計・建造に関係

ご清聴ありがとうございました。