船舶サイバーセキュリティ対策の取り組み アップデート

2021年12月3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**
- ✓ SOLAS条約における国際安全コード(ISMコード)に基づき、船主・運航者は、2021年1月以降の最初の適合証書(DOC)の年次審査までに、現行の**安全管理システム(SMS)でサイバーリスクへの適切な対応を徹底する“ことが求められている。**

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

船舶運航に関する各ファンクションを正常に保つ

■もちろん、船上IT機器も守るべき対象となっている：

例）PCや、そこに含まれる情報：**損傷、改変、悪用**からの保護

衛星通信／無線通信：**傍受、なりすまし、通信妨害**からの保護

■**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**

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

海事分野でのサイバーインシデント事例

■IT機器が対象

①ランサムウェア攻撃による一部システム停止（Maersk/2017年）
②ランサムウェア攻撃による一部システム停止（COSCO/2018年）
③マルウェア感染によるデータセンター被害（MSC/ 2020年）
④ランサムウェア攻撃による一部システム被害（CMA-CGM/2020年）

■OT機器が対象

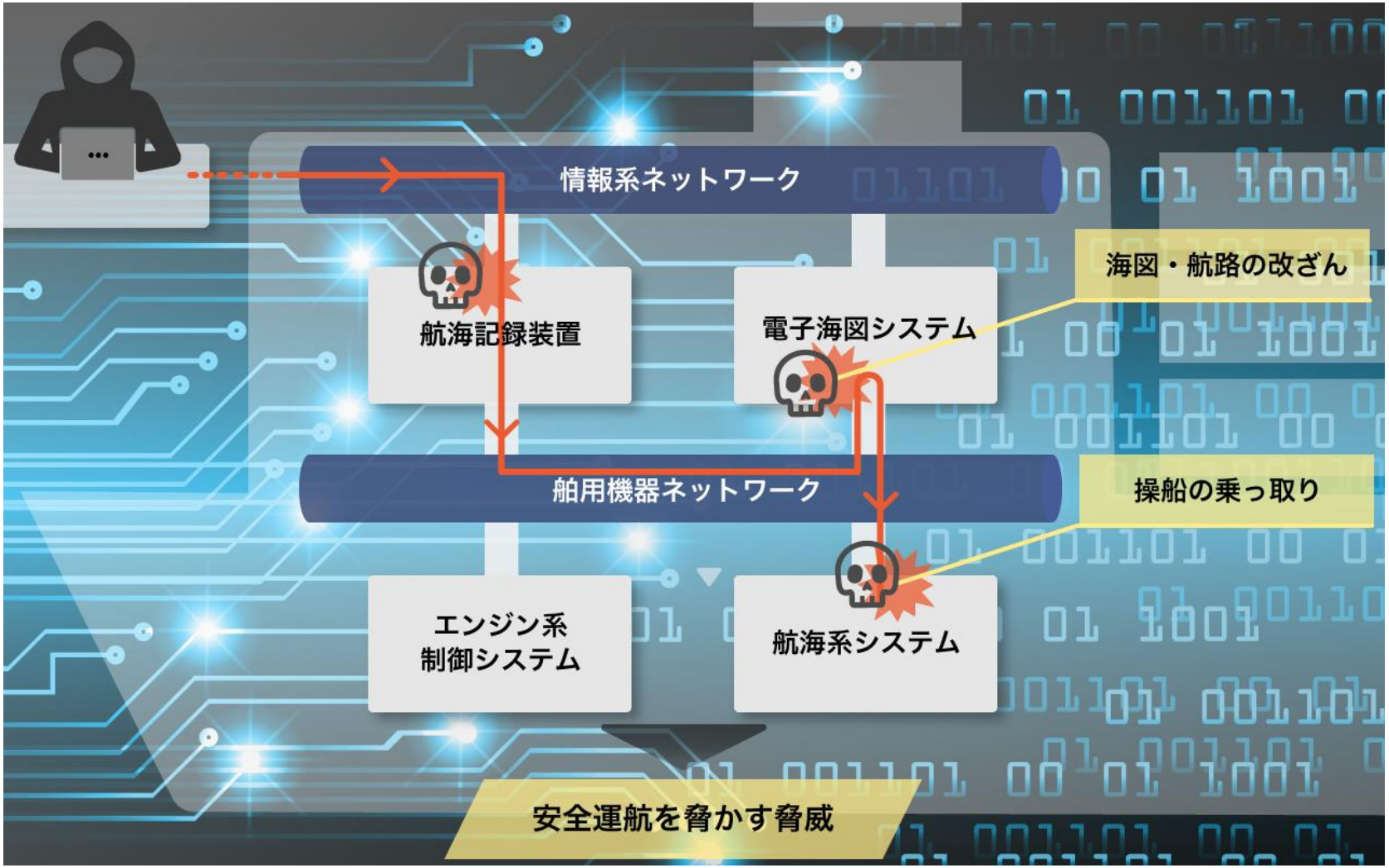
①ハッキングによる操船の乗取り（紅海付近/2017年）
②GPS信号の改ざんによる船舶位置異常（黒海付近/2017年頃から）

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

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

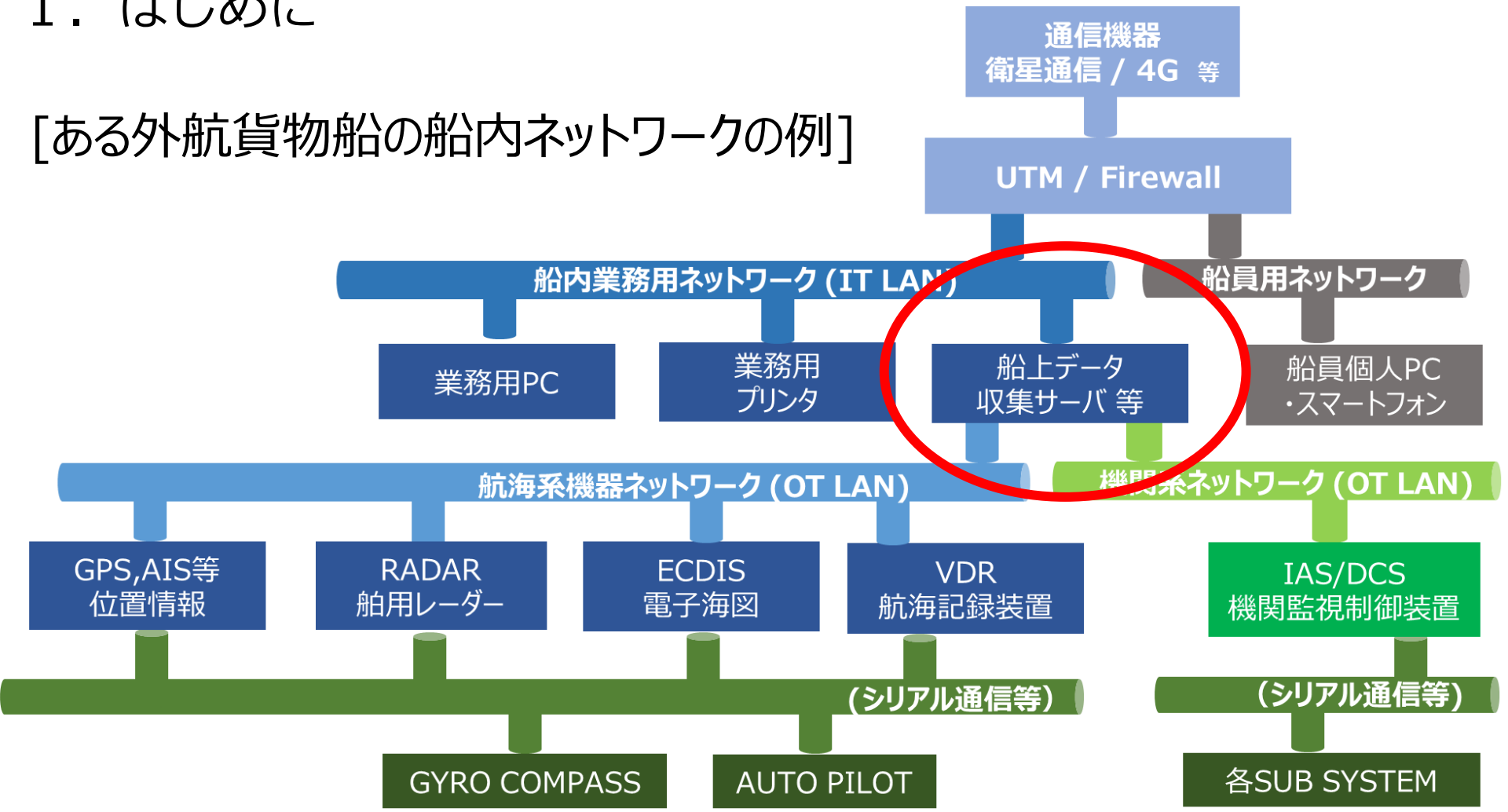
1．はじめに

船舶OT機器への攻撃イメージ



1．はじめに

[ある外航貨物船の船内ネットワークの例]



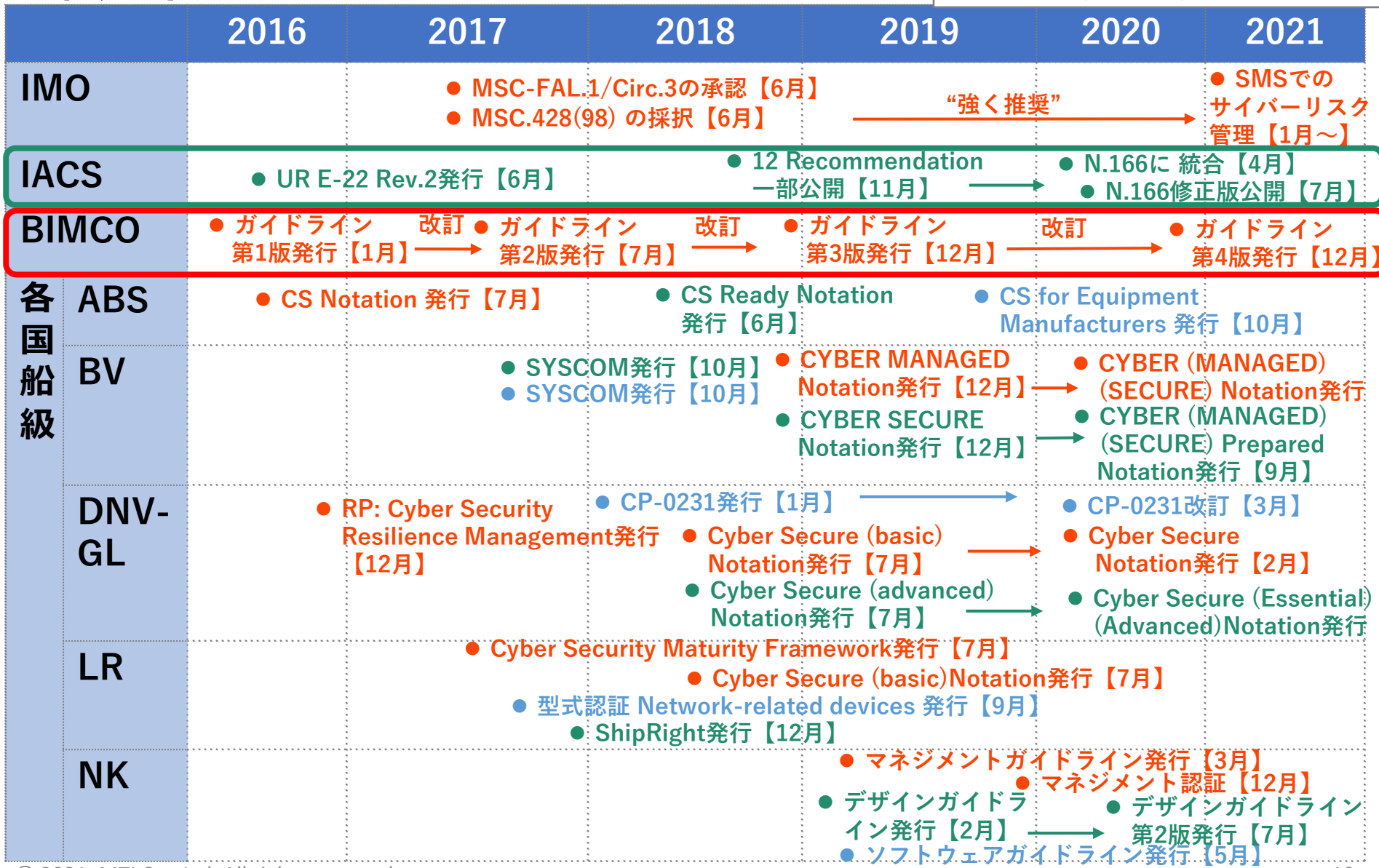
➡船舶データ活用や、船舶自動化が今後進んでいくと、
船舶のOT機器のサイバーセキュリティ対策ますます重要に

目次

2. IMOや各国船級の議論

各種ガイドライン・認証

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



2. IMOや各国船級の議論

BIMCOガイドライン第４版 *1 (2020.12 公開)の目次

*1: 正式名称 "The guidelines on Cyber Security Onboard ships"

2. IMOや各国船級の議論

BIMCOガイドライン 第4版での主な変更点

1.2 Senior management involvement
組織のマネージメントレベルの積極的関与の重要性

1.3 Roles, responsibilities, and tasks
組織全体の関与と連携の重要性

3.2 IT and OT systems' documentation
船会社がリスク管理をするために必要なドキュメント類について明記

5.2 Quantifying the impact
既存のSMSで使用している "Impact scale" の利用を推奨し、サンプル追加

6.1 Relationship between factors influencing risk
リスク要素としての発生率・影響度・脆弱性・脅威の関係を追加

6.3 Third party risk assessments
ペネトレーションテストの利点と注意点について追記

7.2 Technical protection measures
OTシステムのセキュリティパッチ適用の実態と対応について記載

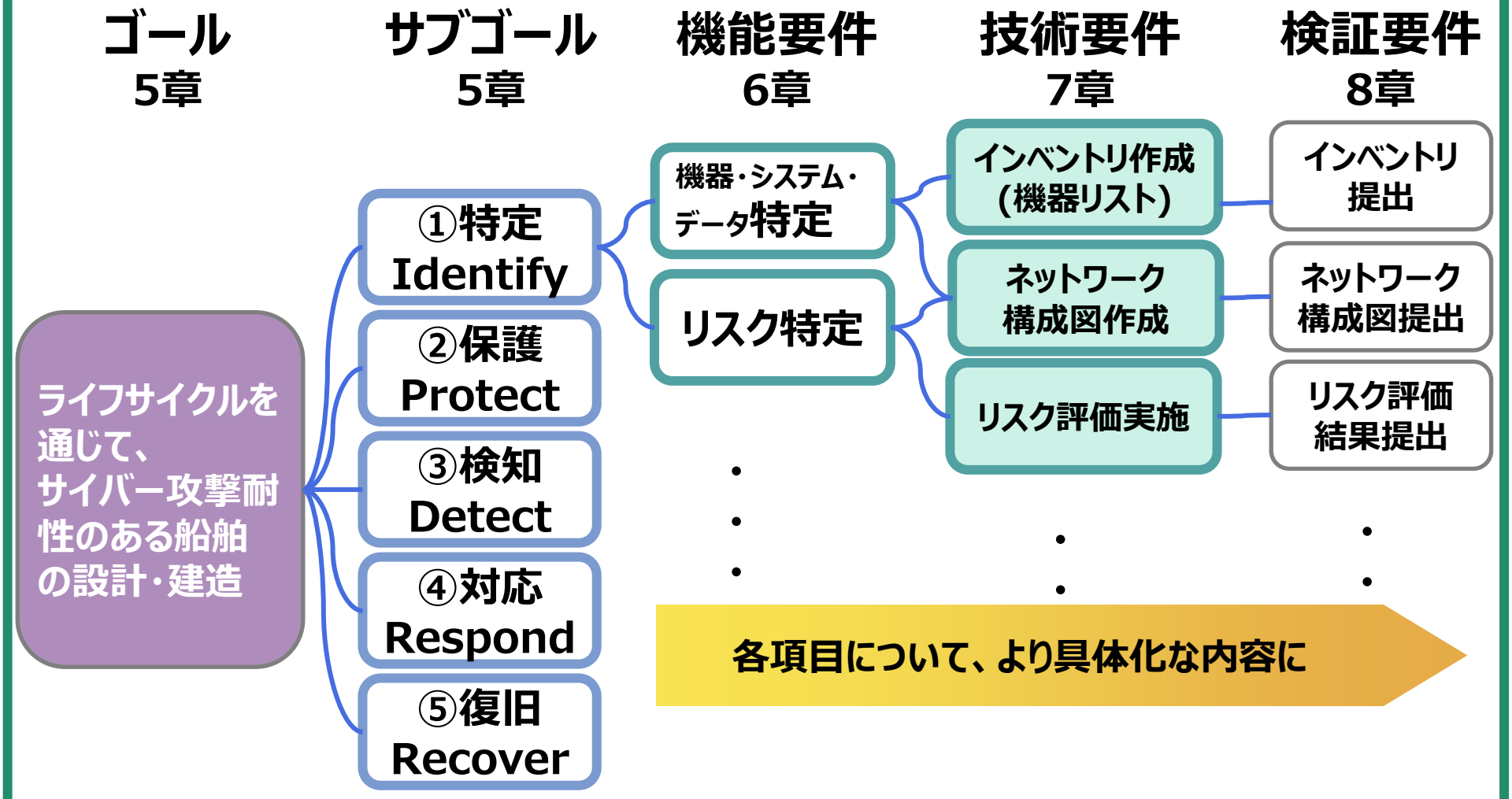
7.3 Procedural protection measures
サイバーリスク管理の教育についてもSTCW条約の要求範囲である事を明記

10.6 Losses arising from a cyber incident
船舶保険のサイバーセキュリティに関する動向について
船主が傭船契約に織り込むべき条項について追加

2. IMOや各国船級の議論

IACS (International Association of Classification Societies, 国際船級協会連合)

推奨事項 No.166：Recommendation on Cyber Resilience (2020年7月)



2. IMOや各国船級の議論

IACS (International Association of Classification Societies, 国際船級協会連合)

IACSメンバーの各船級協会が参加した、Cyber Systems Panel において、船舶サイバーレジリエンスに関する新しい統一規則（UR=Unified Requirement)の策定や、改訂が進んでいる。

1）2020年に公表した推奨事項 No.166 をベースに、“船舶サイバーレジリエンス”に関する新しいURを策定中

2）既存UR E22「コンピュータシステムの船上での利用」も、上記にあわせて改訂中

※年末か来年早々にはこれらURが公表されるとみられている。URは、公表から１年後程度の建造契約の船舶から適用される事例が多い。

2. IMOや各国船級の議論

各種ガイドライン・認証の整理

凡例：船級・各国船級　船技協が実施　個社が実施

		サイバーレジリエンス向上		サイバーリスク管理
	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 サイバーレジリエンスに関する新URとE22改訂		IMO MSC-FAL.1/Circ.3 (2017) BIMCOガイドラインV4 (2020.12)
		各国船級による舶用機器向けガイドライン・認証	各国船級による新造船向けガイドライン・認証	各国船級 船主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発行 (2021年3月)	船技協 CyberResilient Shipガイドライン発行 (2020.3)	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

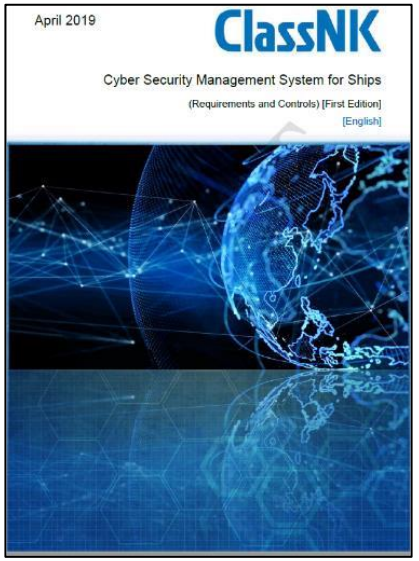
目次

3．船舶運航におけるサイバーリスク管理

NYK運航船における、サイバーマネジメント認証

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

3．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

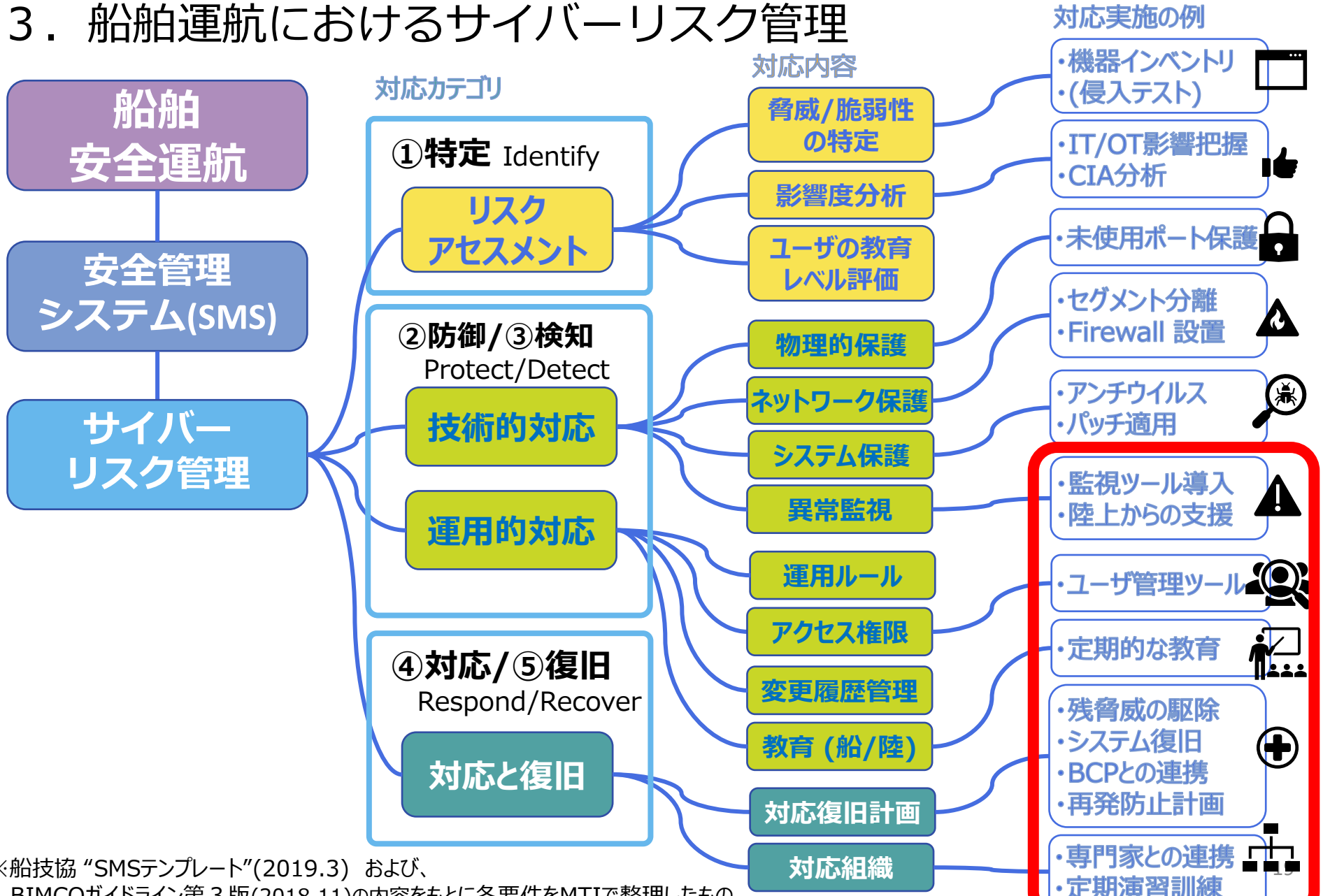
サイバーリスク管理アプローチ：

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)

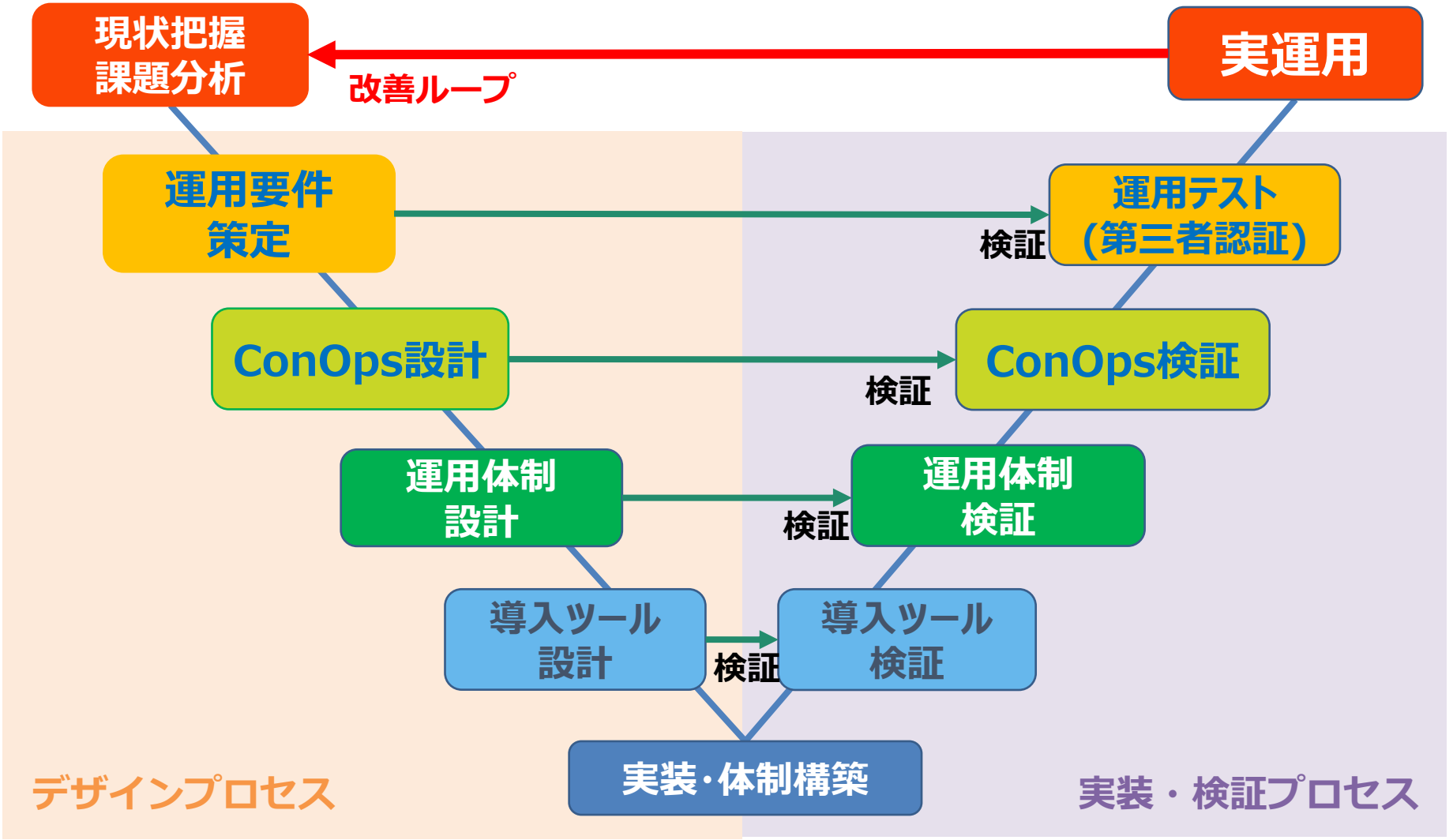
3．船舶運航におけるサイバーリスク管理



※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

3．船舶運航におけるサイバーリスク管理

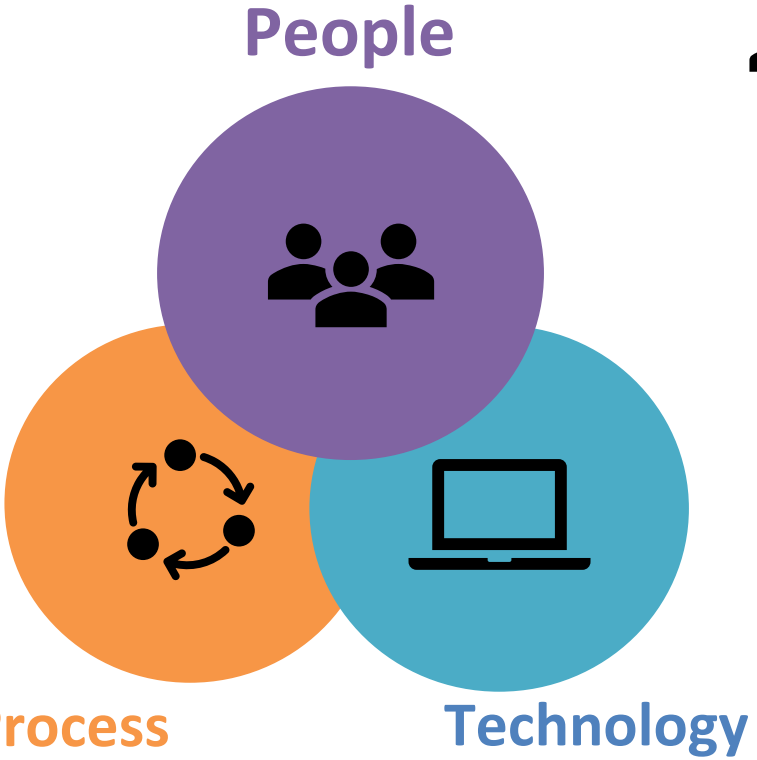
船舶サイバーリスク対策の組織構築におけるV字プロセス



3．船舶運航におけるサイバーリスク管理

ConOps（Concept of Operation）：運用コンセプト

・ユーザの視点から、システムの運用全体を通じた特徴や要求・機能を明確化する文書
・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共通認識を持つ



推奨される実施項目の例

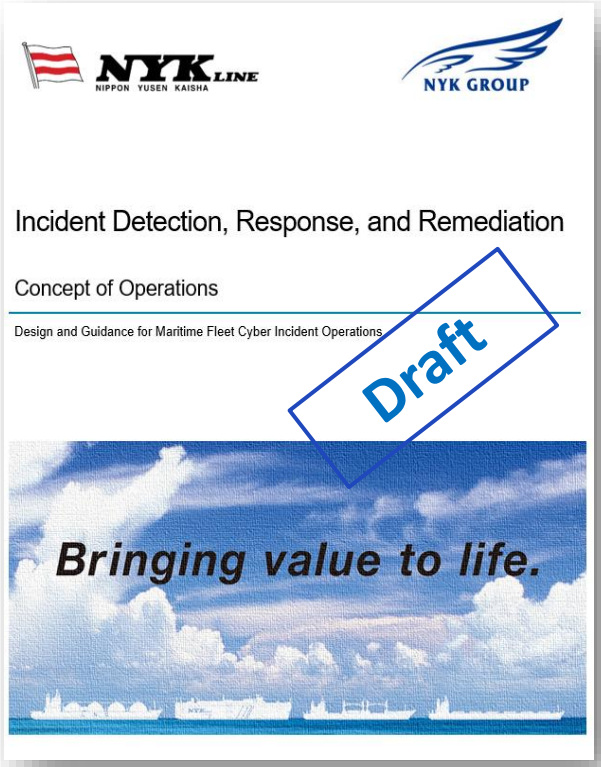
・インシデント検出・対応・修復対応の**組織、人員配置の強化／教育**
・船舶サイバーリスク**モニタリング組織**

・インシデント対応パフォーマンスの**目標値設定、KPI設定**
・ポリシー・プロセスの**定期的な改善**

・**多層的な防御**アプローチの導入
・**OT**ネットワークの**異常監視**
・陸上からの**遠隔監視ツール**の導入

3．船舶運航におけるサイバーリスク管理

NYKにおけるサイバーセキュリティ対応のConOpsを策定



＜主な内容＞

- 背景と目的、スコープ
- 組織設計とガバナンス
  - 推奨する組織体制図
  - 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、スキル、経験
  - RACIチャート（責任分担表）
- ポリシー設計
  - 船舶サイバーセキュリティポリシー
  - 関連サイバーセキュリティドキュメント
  - サイバーリスク管理の対応ポリシー
  - サイバーポリシーの改善
- パフォーマンス管理
  - パフォーマンスの目標値・KPI策定
- 技術/実装
  - Defense in Depthアプローチ
  - IDR&R技術インテグレーション
  - **サイバーリスクのリモートモニタリング**
- ロードマップ

3．船舶運航におけるサイバーリスク管理

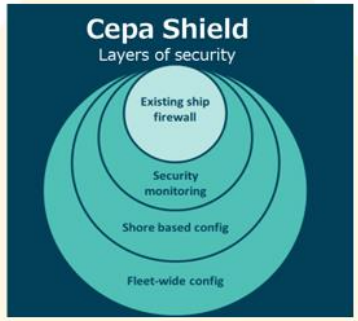
船舶サイバーリスクのリモートモニタリング

4. NYKグループにおけるこれからの取り組み②

NYK LINE NIPPON YUSEN KAISHA
株式会社 MTI Monohakobi Technology Institute

・機能要件の立案検討
・50隻での搭載トライアル
・機能評価フィードバック
・UI/UXに関するフィードバック
・搭載ならびに運用に関するパートナー体制の構築
など

Innovation Norway



dualog
Your digital platform at sea

・詳細要件・技術デザイン
・機能開発と改善
- 船上システム
- 陸上モニタリングシステム
- 陸上データ解析システム
- 陸上からの船上機器設定管理
- フリート全体の機能管理
など

ノルウェーの政府系ファンド「Innovation Norway」から2年間の資金援助を受け、Dualog社と共同で、船舶向けサイバーリスク管理システムの開発に関するプロジェクトを開始 (2019年11月21日プレスリリース)

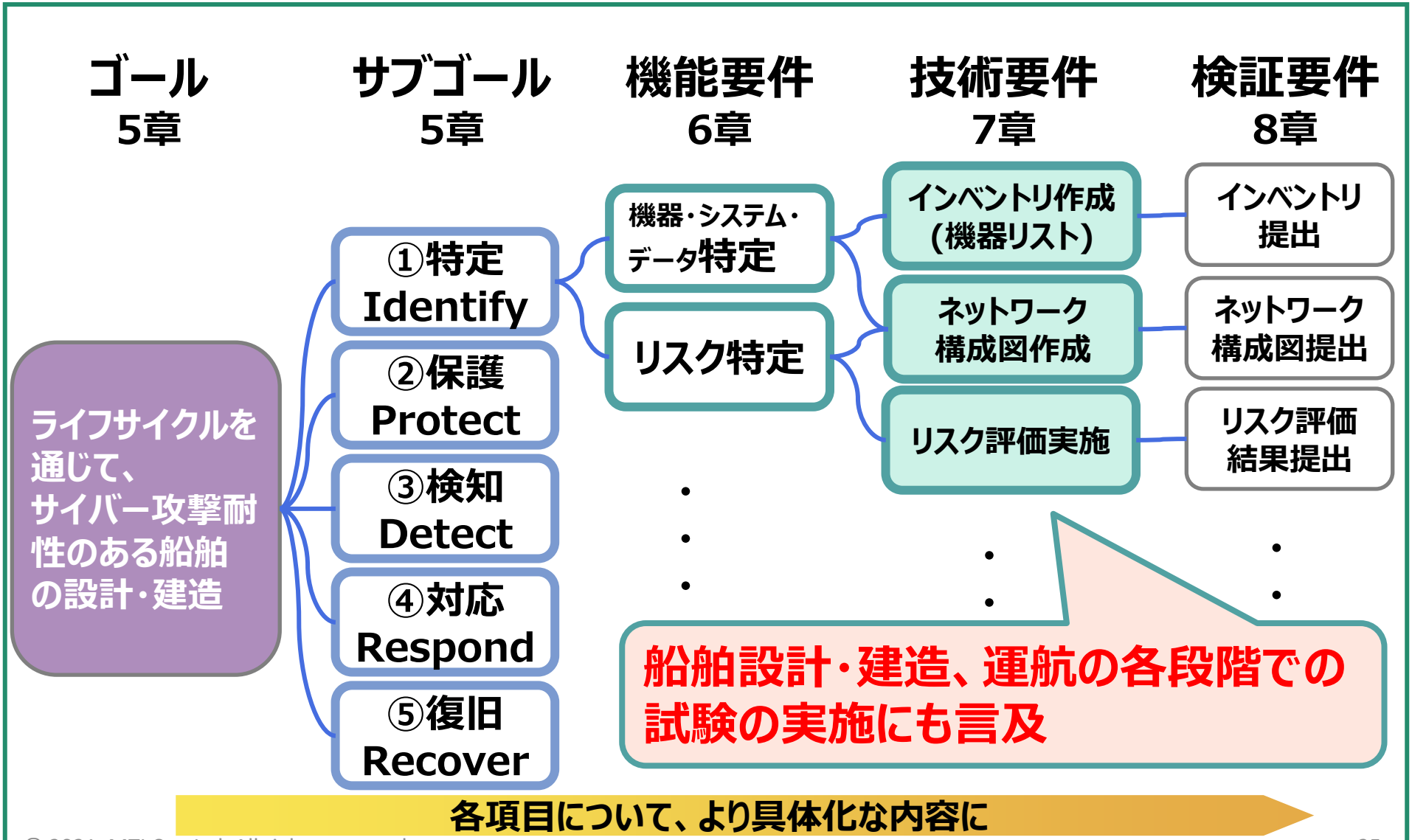
抜粋：2019年 Monohakobi Techno Forum 柴田発表資料より

➡船上サイバーリスク監視に関するツール導入および陸上監視対応体制の準備を進めている

目次

４．船舶サイバーレジリエンス向上

IACS Recommendation on Cyber Resilience No.166



4．船舶サイバーレジリエンス向上

現時点では船舶へのサイバー耐性試験(ペネトレーションテスト/PT)を**義務付けているガイドラインやNotationはない**が、今後、**ハイリスク船や自律運航船**などでは、**実施が求められていくと考える**

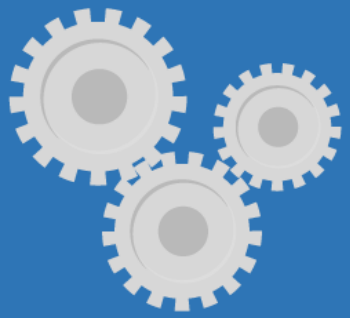
組織名	IACS	ABS	DNV	BV
文書名	IACS Recommendation No. 166 “Recommendation on Cyber Resilience”*	CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES ABS CyberSafety™ VOLUME 2**	DNVGL-RU-SHIP “RULES FOR CLASSIFICATION Part 6 Additional class notations Chapter 5 Equipment and design features”***	NR 659 DT R00 “Rules on Cyber Security for the Classification of Marine Units”****
Notation	(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**

4．船舶サイバーレジリエンス向上

運航者視点で、安全運航に影響を与えるサイバーインシデントを定義し、その脅威の顕在化を目的とした「**脅威ベースペネトレーションテスト(TLPT)***1 」の実施が有効

脅威ベースペネトレーションテスト（TLPT）

ソフトウェア/ハードウェア機能



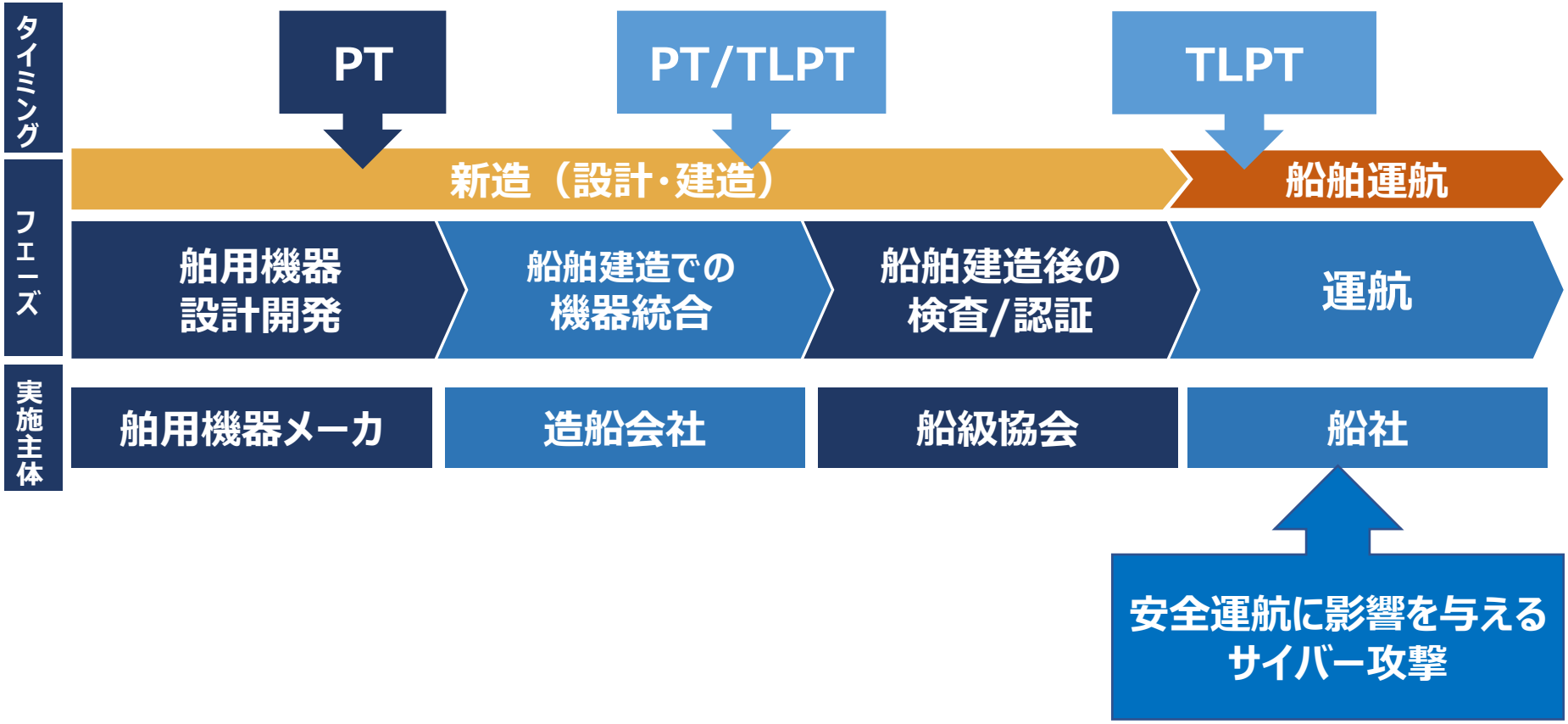
規則・手順

人・組織的対応

*1 TLPT = Threat Led Penetration Test

4．船舶サイバーレジリエンス向上

PT/TLPTを実施するタイミングは、機器設計開発、新造船建造、運航時と、**それぞれのフェーズで適した試験方法**がある。また、結果評価や改善策の策定には、**サイバーセキュリティ専門家との連携も重要**



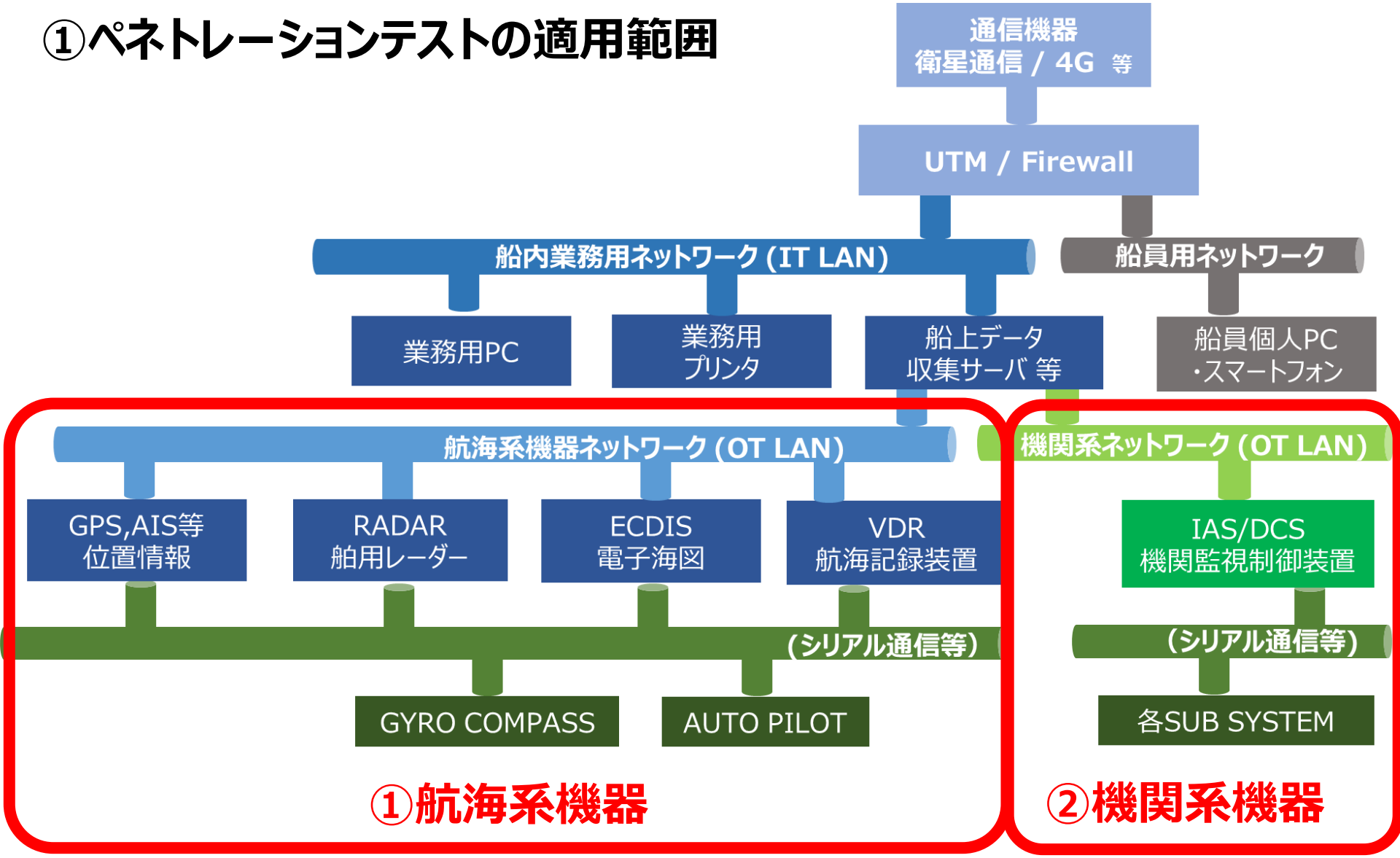
4．船舶サイバーレジリエンス向上

NYK/MTIでは、業界各プレーヤと連携し、サイバーセキュリティ専門家の協力を仰ぎながら、PT/TLPTの手法検討と課題抽出を目的とした、模擬船舶環境でのトライアルを実施（2020年）

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	

4．船舶サイバーレジリエンス向上

①ペネトレーションテストの適用範囲



４．船舶サイバーレジリエンス向上

②トライアルの結果と成果

- ✓ 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

③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が必要 (When/Who/How)

➡ **海運ビジネスとしての実施コスト/メリットも考慮して船級を含めた業界内での合意形成が必要**

目次

5．まとめ

1．IMOや各国船級の議論

- ✓ BIMCOガイドライン第4版は、さらに業界の実態に即した内容に改訂され、**運航者のサイバーリスク管理に限らず、造船所やメーカにも有用なものに**
- ✓ IACSでは、No.166 の推奨事項をベースに、船舶サイバーレジリエンス向上に関する、**統一規則（UR）策定と、UR E22の改訂**を予定。

2．船舶サイバーリスク管理

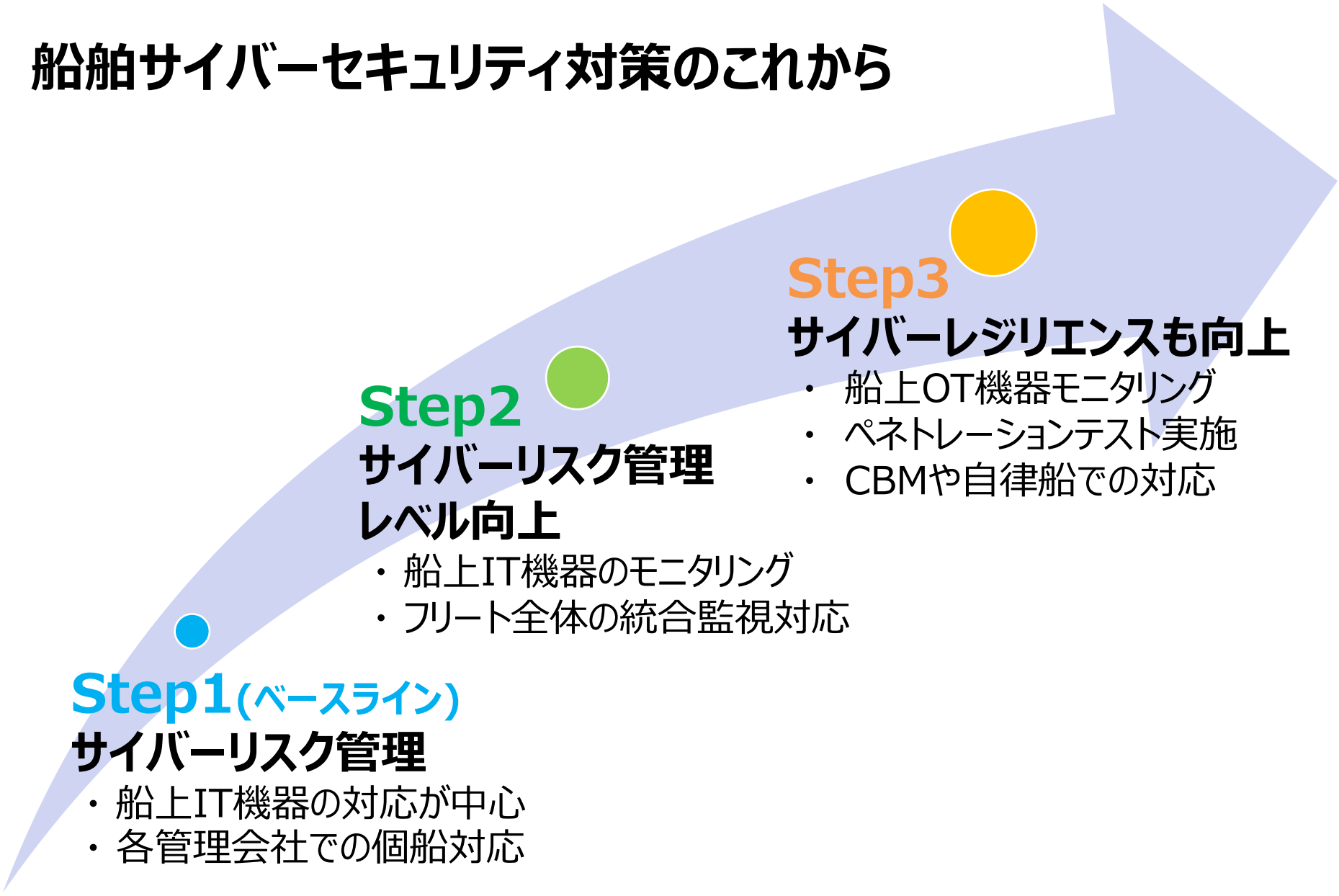
- ✓ 2021年1月以降、運航者の**SMS(安全管理システム)での対応が進む**
- ✓ さらなるレベル向上には、「特定・防御」だけでなく**「検知」「対応」「復旧」が重要**
- ✓ 「組織」「プロセス」「技術」を網羅した**ConOps(運用コンセプト）**がまず必要
- ✓ NYKでは**陸上での統合監視と即時対応の仕組み・体制**を準備中

3．船舶サイバーレジリエンス向上

- ✓ ペネトレーションテストは**有用であるが、実施ポイント・方法の業界議論**が必要
- ✓ 今後、**自律船やCBM等の高度船舶では、さらなる対応が要求**されてくる

5．まとめ

船舶サイバーセキュリティ対策のこれから



Step1(ベースライン)
サイバーリスク管理
- 船上IT機器の対応が中心
- 各管理会社での個船対応

Step2
サイバーリスク管理レベル向上
- 船上IT機器のモニタリング
- フリート全体の統合監視対応

Step3
サイバーレジリエンスも向上
- 船上OT機器モニタリング
- ペネトレーションテスト実施
- CBMや自律船での対応

ご清聴ありがとうございました。