船舶のサイバーセキュリティ対策 ～IACS UR E26,27の要求・課題と、海事業界で必要とされる取り組み～

2023年12月4日

株式会社MTI　船舶物流IoTチーム
橋本 仁

標準・規格の流れーIMOや各船級の議論

海事業界のサイバーセキュリティ規格・ガイドラインも整備が進んでいる。

2019 取得任意

各船級
「ガイドライン」「ノーテーション・認証」発行
(NYK) LNG船のノーテーションをClass NKやBVから取得

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。
（NYK）ー サイバーリスク管理ポリシーを発行
ー SMSに基づくリスク管理・対策実施

2024/7～ 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**（Unified Requirements)発行。
UR E26: Cyber resilience of ships
UR E27: Cyber resilience of on-board systems and equipment
対象　**2024/7/1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ーフェース

IACS UR E26/E27概説

IACS UR E26, E27とは

船舶・人命・積荷の安全な航行実現のために、サイバー攻撃への対応が船舶建造段階で求められている。
2024年のうちに**新造契約船に対する強制要件**※として発効される見込み。

	E26 船舶のサイバーレジリエンス	E27 船上システム及び機器の サイバーレジリエンス
主体：フェーズ	船主：船舶運用	造船所：船舶建造 / メーカー：機器製造
対象	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、識別・防御・検知・対応・復旧の側面からセキュリティ要件を定義。	**機器メーカー**による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（**識別・防御・検知・対応・復旧**） 5. パフォーマンス評価とテストプラン 6. 適用除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. 船級への提出書類 4. システム要件 ・ **セキュリティ capability** ・ **追加セキュリティ capability** 5. 製品設計・開発要件 ANNEX　関連UR (E10,22,26) ,参考文献

※既存船に対するサイバーセキュリティ要件は船級ごとに独自で制定

E26概説

目的

- サイバーレジリエント船実現の技術的手段(最小要件セット)をステークホルダーに提供
- E10, E22,E27などを補完的に適用するための「ベース※1」

適用範囲

OTシステム	データを使用して物理プロセスを制御/監視するCBS※2 かつ 機能中断や障害が運航に影響あり得るOTシステム	①推進 ②ステアリング ③投錨・係留 ④発電・配電 ⑤火災検知・消火 ⑥CMS(荷役システム) ⑦ビルジ/バラスト/積下ろし制御 ⑧ボイラー制御 ⑨スクラバー関連 ⑩水密完全性と浸水検知 ⑪照明 ⑫法規制準拠の航海/通信システム ⑬その他
上記CBS間のIPベースの通信インターフェース機器		・管理者向けネットワーク ・客/訪船者サービス・管理システム ・客向けネットワーク ・船員福利厚生システム ・OTにつながるその他のシステム(恒久的/一時的なもの問わず)

適用除外項目

- NAV/COM等はIEC61162-460/63154※3で代替可能
- 「サイバーレジリエンス能力」要件と同等以上である事の提示必須

※1 搭載システム及び機器のサイバーレジリエンス要件はUR E27に記載。
UR E10：船舶搭載機器の型式承認規格
UR E22：オンボードCBSの設計・構築・試運転及び保守に関する要件

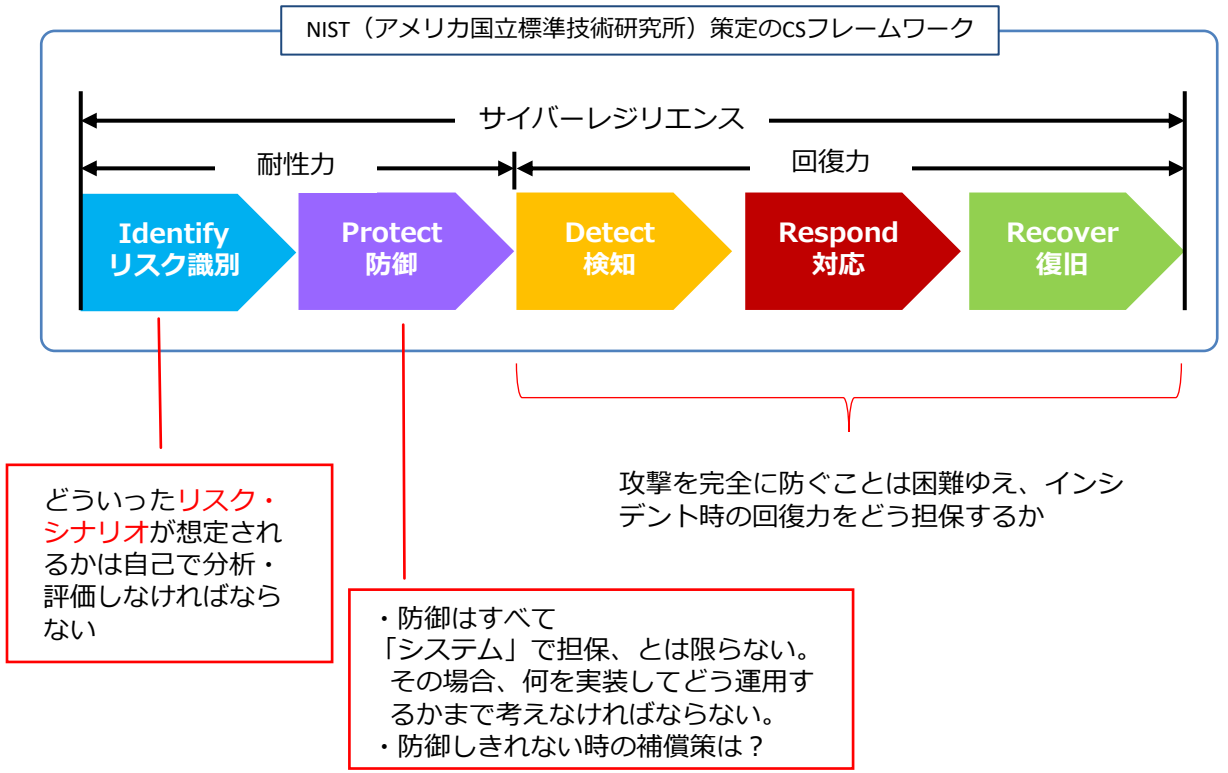
※2 Computer Based Systems
※3 IEC61162-460/63154: 無線及び航海計器デジタルインターフェース規格

E26概説

- ゴールは船のサイバーレジリエンスの実現。これを５つのサブゴールに分解、それぞれの要件を達成する
- 但しE26はあくまで**一般的な要件ガイドライン**。リスクと防御手段（システムや人）の策定、回復までのシナリオは運用側がイメージして詳細まで落とし込む必要がある

サブゴールごとの達成要件

Identify	アセットインベントリ（とリスクアセスメント）
Protect	セキュリティゾーン
	ネットワーク保護
	マリシャスコード対策
	アクセス制御
	無線通信
	Untrusted Networkからのアクセス制御
	モバイルやポータブル端末利用制限
Detect	ネットワーク監視
	ネットワーク及びシステム診断
Respond	インシデント対応計画
	ローカル/単独/手動操作
	ネットワーク分離
	フォールバック（縮退運用）
Recover	復旧計画
	バックアップ・リストア能力
	制御されたシャットダウン/リセット/ロールバック/リスタート



E27概説

E27は搭載システム技術要件

技術要件	基本要求※1
未承認の意図的または偶然の**アクセスに対する防御**	IEC62443-3-3 FR 1
意図的または偶然の**誤操作に対する防御**	IEC62443-3-3 FR 2
意図的または偶然の操作に対する**CBS完全性の保護**	IEC62443-3-3 FR 3
盗聴または意図的な暴露を経た、**未承認の情報公開の防止**	IEC62443-3-3 FR 4
CBSの**操作の監視とインシデントへの対応**	IEC62443-3-3 FR 6
制御システムが**通常の運用条件下で確実に動作することの保証**	IEC62443-3-3 FR 7

セキュア開発ライフサイクル(SDLC)要件　IEC62443-4-1※2

- 但しIEC62443-3-3に記載された「すべての要件」が要求される訳ではない
- システムのゾーン内で機能を満たせば、各CBSが全て同じ機能を持つ必要はない
(特に一部のネットワーク監視・アクセス制御機能など)

※1具体的な要件は、IEC62443-3-3に記載の「SR」相当について
・必要なものだけ要求
・システムとして要求が当てはまらないCBSについては「該当しない」ことを示す
※2メーカーの開発体制に関する、ごく一部の要件が適用

可用性、運航継続性、補償可能性が成立することが前提要件

前提要件	
可用性	システムが障害などで停止すること無く稼働し続けることで、障害点の影響や停止が全体におよぶことのないようにする。
運航継続性	あらかじめ用意した縮退シナリオで、最低限運航を担保する。
補償可能性（E26）	仮にゾーン内でE27機能を満足できない場合、船員行動や船内オペレーションに追加対策を施す (E26による補償)で対応できる場合がある (船級と協議が必要)。

CSリスク・シナリオ例 (運航への脅威と対策：GNSS)

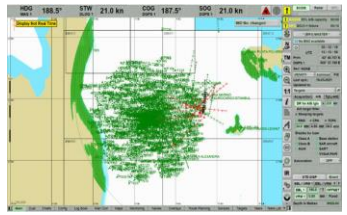
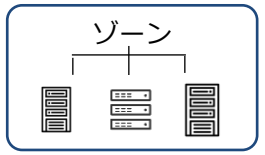
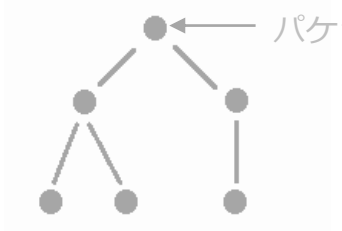
E27非対応の要件について補償策対応要件についてもサブゴール達成シナリオを構築

この中で、E27要件についての〇×を決める

基本機能	脅威の検討	攻撃パターン			対策		関連する対策(IACS UR)		その他対策
GNSS	運航に影響	内容	経路	技術	本体側(IEC難易度)	ゾーン内対策(IEC難易度)	E26	E27	
自船位置、時刻などの航海情報を提供		偽電波発信	船外→アンテナへ電波放射	難	**電波の真偽判定(SL3~4)**	ー	ー	ー	電波妨害対策
	スプーフィング ↓ 間違った自船位置情報をもとに、誤った航行を誘導	データ改ざん	機器の処理部へ直接(REDS/NW経由)	易~中	**REDSアクセス対策(SL2)** **NWアクセス対策(TCP/IP→SL2、それ以外はSL3~4)** データ完全性判定(SL2)	**ゾーン内各機器でデータ完全性判定(SL2)**	**全てのサブゴール施策**	**SR1.1,1.3, 1.4, 1.5, 1.7, 1.10, 2.1 SR1.6,2.2, SR2.3, SR2.4, 3.2, SR2.8, 2.9, 2.10, 2.11, 6.1 SR3.1, 4.1, 4.3, SR3.3, 3.6 SR7.2 ~ 7.7**	
			NW内のノードから偽データを流す	易~中	ー	**パケット監視→データ完全性判定(SL2)**	**セグメント化/NW保護 Maliciousコード対策 アクセス制御** 無線通信 **NW監視/診断 NW分離・フォールバック 復旧計画 バックアップ・リストア 制御された復旧**	**SR1.6,2.2, SR3.1, 4.1, 4.3,**	
	位置データ出力不能 ↓ 位置が示されなくなり、航行不能に	DoS攻撃	DoSコマンド(REDS/NW経由)	易~中	**REDSアクセス対策(SL2) NWアクセス対策(TCP/IP→SL2、それ以外はSL3~4) DoS攻撃対策(SL2)**	パケット監視→DoS攻撃対策(L2)	**全てのサブゴール施策**	**SR1.1,1.3, 1.4, 1.5, 1.7, 1.10, 2.1 SR1.6,2.2, SR2.3, SR2.4, 3.2, SR2.8, 2.9, 2.10, 2.11, 6.1 SR3.1, 4.1, 4.3, SR3.3, 3.6 SR7.1 ~ 7.7**	
			乗っ取り(REDS/NW経由) →機能停止	易~中	**REDSアクセス対策(SL2) NWアクセス対策(TCP/IP→SL2、それ以外はSL3~4)**	パケット監視→DoS攻撃対策(SL2)		**SR1.1,1.3, 1.4, 1.5, 1.7, 1.10, 2.1 SR1.6,2.2, SR2.3, SR2.4, 3.2, SR2.8, 2.9, 2.10, 2.11, 6.1 SR3.1, 4.1, 4.3 SR3.3, 3.6 SR7.2 ~ 7.7**	
		シャットダウン	乗っ取り(REDS/NW経由) →シャットダウン	易~難		パケット監視→DoS攻撃対策(SL2)			

SL: Security Level
SR: Specific Requirement
REDS: Removable External Disk System

CSリスク・シナリオ例　GNSSスプーフィング

被害リスク	侵入経路	対策
 自社船・他社船の正確な位置がECDIS上見れない →航行に影響	NWやUSBから機器へ直接攻撃	NW ゾーン単位で障壁があれば、個々の機器のNW I/F対策は必須ではない、とする※  USBなど着脱可ストレージアクセス制御 (挿しても認識しない、Autorunしないなど）あれば可、とする※ **※というリスクアセスメントをした場合の例**
・・・	NW内ノードから偽情報	

E26（船主/造船）

識別・防御・検知
・ゾーン単位の障壁確保
・ログ監視、アラート機能
対応
・不審な通信のブロック
・汚染ブロック切り離し
・マニュアル航法へ切替
・バックアップ起動
復旧
・システムバックアップ
・汚染ブロック正常確認
・再起動

対策シナリオベースに機器側の対応要否を検討

・・・
・・・

E27（メーカー）

○/x	詳細要件	SR
	人間ユーザーの識別と承認	1.1
	アカウント管理	1.3
	識別機構管理	1.4
	承認機構管理	1.5
	ワイヤレスアクセス管理	1.6
	パスワードベース承認	1.7
	承認機構の応答	1.10
	承認の強制	2.1
	ワイヤレス使用の制御	2.2
	REDS使用の制御	2.3
	モバイルコード	2.4
	監査イベント(の定義)	2.8
	監査情報のストレージ要領	2.9
	監査処理失敗時の応答	2.10
	タイムスタンプ	2.11
	通信の完全性保護	3.1
	セキュリティ機能の検証	3.3
	仕様に基づいた出力	3.6
	通信の機密性	4.1
	暗号化技術の使用	4.3
	監査ログのアクセシビリティ	6.1
	リソース管理	7.2
	システムバックアップ	7.3
	システム回復	7.4
	代替電源	7.5
	ネットワーク・セキュリティ構成設定	7.6
	最小機能	7.7

運航側が想起するCSリスク・シナリオ例

こうした事象・攻撃は起こり得るのか、起こり得るとしてその対策・対処は？
運航、機器両方を理解する必要性

- 主機の表示と実際が逆転する（BridgeではAhead表示なのに実際はAsternに回っている）
- 操舵機が片方だけおかしくなる
- 一度Stop Engineにした後、次に主機を起動する際にAhead/Asternがランダムになる

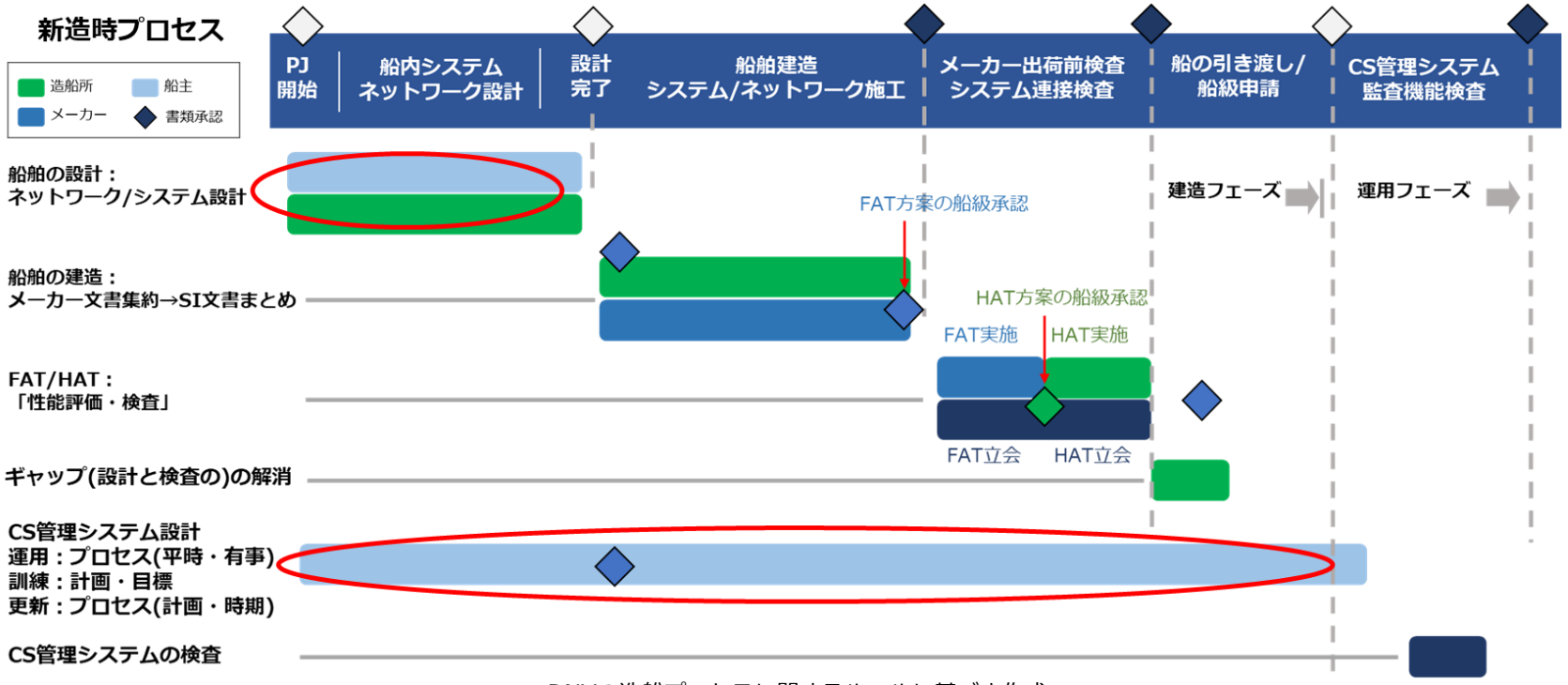
  → 座礁・衝突リスク、出入港時に混乱
- 主機の回転数が一定以上あげられない

  → 進めるがスケジュールが守れない
- ECDISの挙動が明らかにおかしい

  → 1台だけでもルール上入港できない

E26/E27対応における課題

- あくまで一般ルールであり、「要件を満たせば100%サイバーセキュア」なわけではない
- IACSの「サイバーレジリエンス実現に必要な具体的対策とその根拠」に明確な規定はない
- どの船級もIACSに沿った要件は課すものの、要件に書かれていないルール（年検スケジュール、リスクアセスメント方法の明記など）は独自に決めるケースが多い

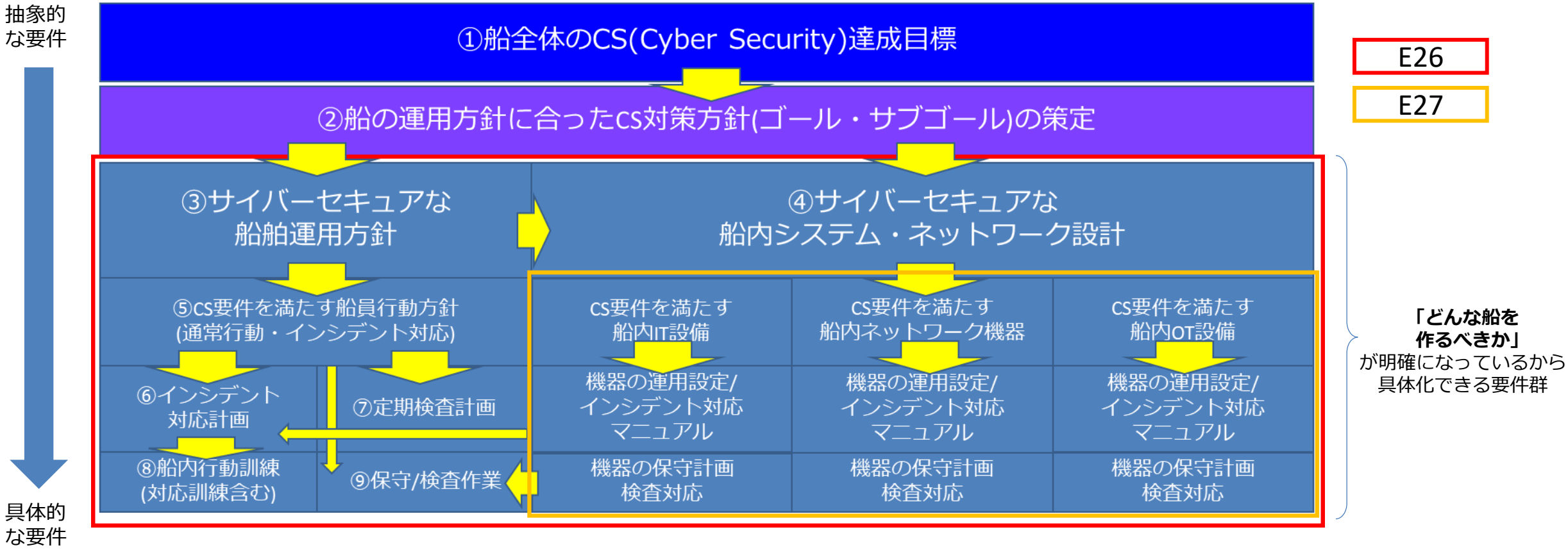


DNVの造船プロセスに関するルールに基づき作成

船の「コンセプト設計」の段階で、すでにサイバーセキュリティの方針が定まっている必要がある。

NYK/MTIが考える、船のコンセプト設計プロセスにおけるCS要件のとらえ方

E26/27と「サイバーレジリエントな船を作るためのコンセプト設計」の関係

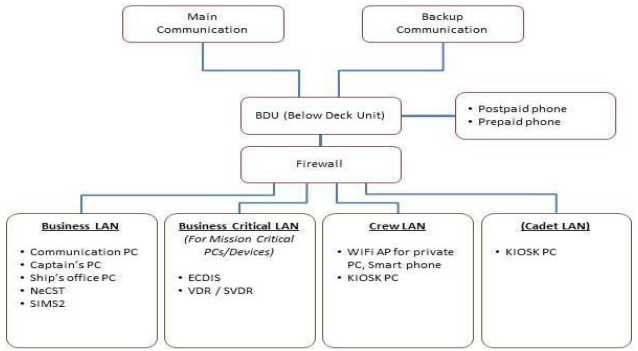


船の要求元が「どんな船を作りたいか」に基づいてCS達成目標を決めることで、
E26/E27の要件＋αを具体化し、関係各社・船級と意識を共有して解決する。

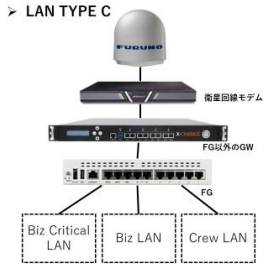
NYK/MTIの取り組み

NYK/MTIの船上データ利用の取り組み足跡

2012年から始まるSATCOMプロジェクト（VSAT通信導入と船内LAN構築）を皮切りに、SIMS２プロジェクト（船舶IoTデータ収集と活用）を経て、船陸間データ伝送・共有の安定化/効率化と、業界のフロントランナーとして取り組んできた。



通信システム刷新と船内LAN基準

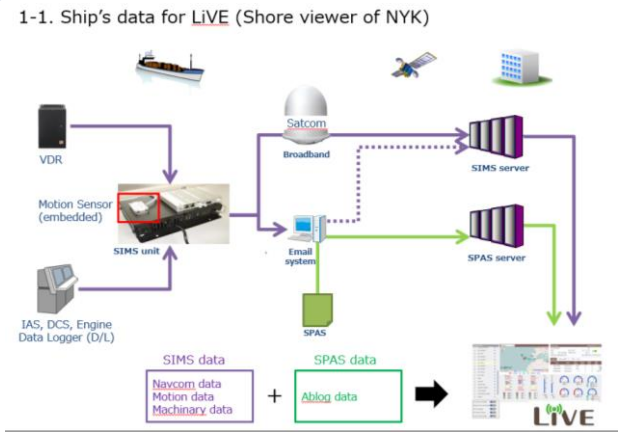


2012年～ SATCOMプロジェクト

2008年
SIMS１プロジェクト開始

1999年後半
舶用EMAIL導入

2014年～SIMS２プロジェクト

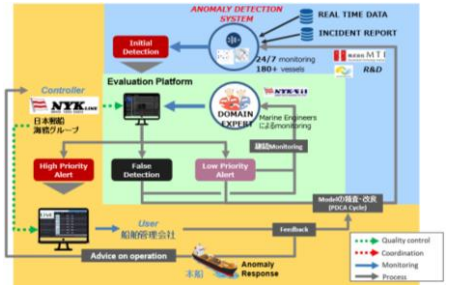


2017年～ Dualog協業開始

2017年～
安定的・効率的・安全な
船陸間データ伝送・共有ドライブの開発

2019年～
統合的なサイバーリスク監視の開発

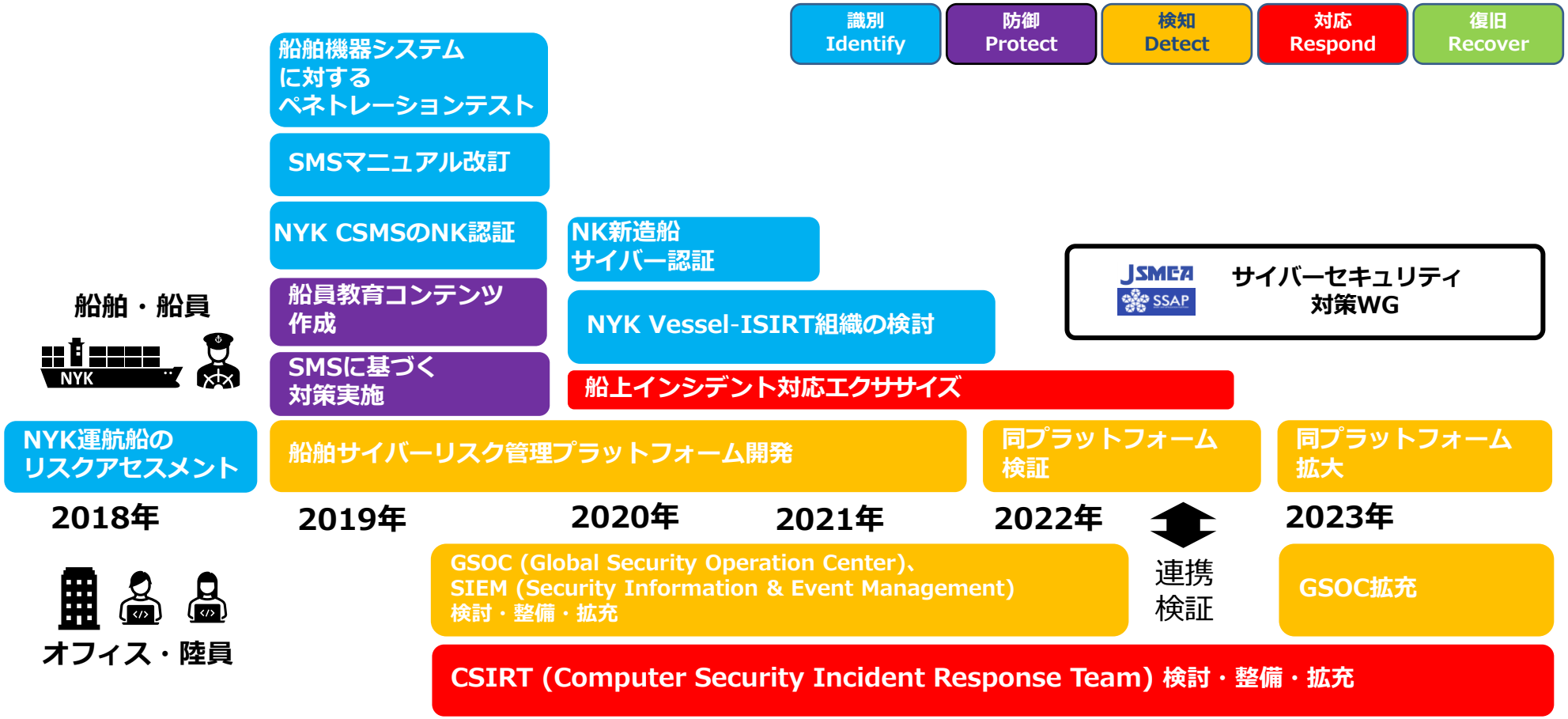
次の段階へ



14年～16年　100隻搭載開始とデータみえる化LiVE実装
17年～　傭船展開開始と機器異常検知ロジック開発
20年～　RDC運用開始

NYK/MTIの船舶向けサイバーセキュリティの取り組み足跡

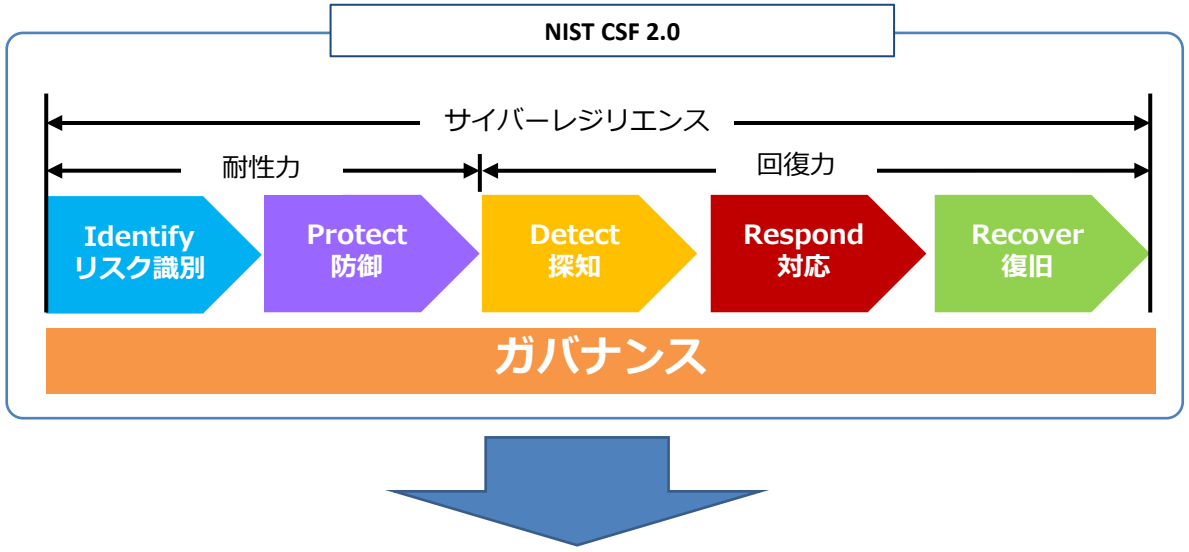
「つながる船」によるサイバーリスクの高まりを受け、NISTベースでの様々な取り組みを実施。



NYK/MTIの「サイバー攻撃に対応できる船」の考え方

最新のNISTフレームワークにはガバナンスが追加。

- 各機能の成果に対して、事業戦略に基づく優先順位付けをサポートするもの
- ガバナンスにはサプライチェーンやソフトウェア開発、AIに関するリスクマネジメントフレームワークなどが参考情報として追加されている



「どんな船を作り、運用するか」に基づく
就航後の行動計画の立案(ガバナンスの確立)
が、CS達成目標のための**屋台骨**として重要

・船員がサイバーセキュリティの知識を持ち、
・適切なレジリエンス能力を持ったシステムを導入し、
・正しくレジリエントな船/陸上支援の運用を実施して、

初めてサイバー攻撃に対応できた、といえる。

今後取り組むべきこと

- 「サイバーレジリエンスの獲得」実現には、
  「運用方針」について設計段階で船主・造船所・メーカー間の合意が不可欠
- この延長線上には自律運航船も
- 既存船への対策も引き続き必要※

スマナビ研における活動

- MTIはスマナビ研のサイバーセキュリティ対策WGにおいて、IACS UR E26/E27を始めとした規制・規格動向をメンバー各社と共有、対応を協議している
- NYK/MTIは、様々な船級や研究機関と情報・意見交換しながら船主/船社としての総合的なCRガイドライン策定を予定しており、こうした情報の共有も行っていく。
  また、一度作れば終わりではなく、実際のインシデントや脅威の高度化を受けて随時更新が必要であり、こうしたトピックも扱っていく
- スマナビ研では、広島商船高専を始めとした内外の学術・研究機関等と提携し、
  船員向けCSリスク・対応教育コースの作成や、ペネトレーションテスト施設の整備、
  船上でのサイバーアタック演習など、会員向けプログラムを充実していく予定

※非強制要件ではあるが、近々IACSから既存船に対するCS対策Recommendationが発翰される見込み

スマートナビゲーションシステム研究会（Smart Ship Application Platform (SSAP) Project　https://www.jsmea.or.jp/ssap/jp/

ご清聴どうもありがとうございました。