船舶におけるサイバーセキュリティ対応の現状とこれから

2019年11月25日　東京会場
2019年11月29日　広島会場

株式会社MTI　船舶物流技術グループ
柴田　隼吾
Jungo Shibata

目次

1．はじめに

船舶のシステムインテグレーションにおける

“サイバーセキュリティ” とは？

引用：Shipping 4.0 ,SINTEF OCEAN,2017

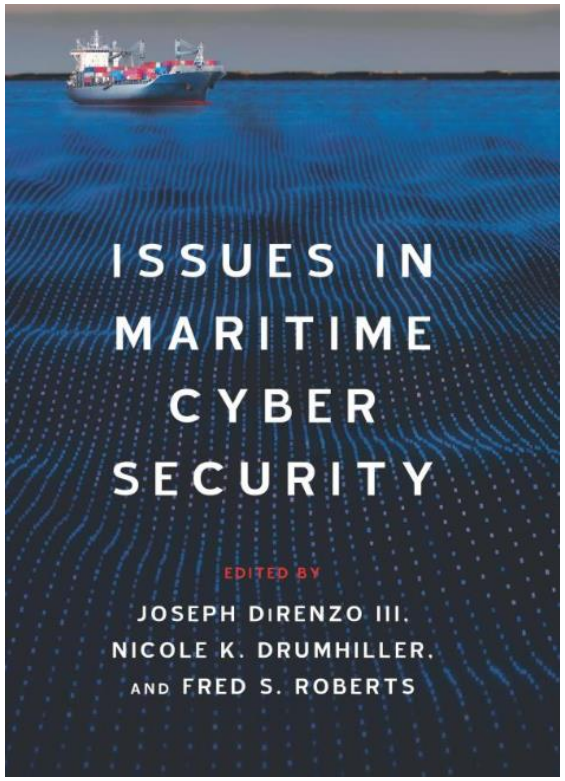
1．はじめに

- ✓ 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。

“Recomandatory”

※2021年１月以降の最初の年次検査までに

2．海事分野でのサイバーインシデント事例①



出典：Issues In Maritime Cyber Security
Westphalia Press社,Sep.2017

ケース1：「船舶ナビゲーションシステムの混乱」

2013年、テキサス大学オースティンの学生が、**GPS信号を偽装(Spoofing)**し、ヨットの**自動操舵を乗取り**、遠隔から誤った航路に変針する実験に成功

ケース2：「ハッカーが港湾施設を介して薬物密輸」

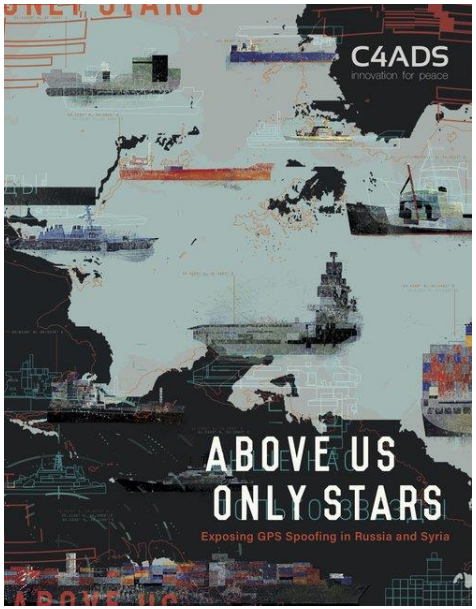
2011年から 2年間、アントワープ港では密輸業者がハッカーを雇い、**違法薬物を南米バナナや木材のコンテナの情報に書き換え密輸**されていた。

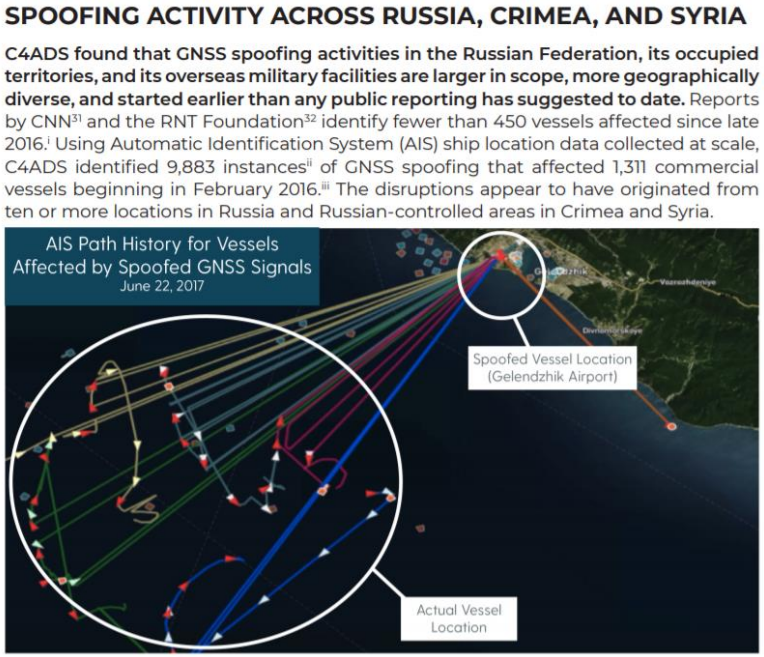
ケース3：「サプライチェーンに侵入するマルウェア」

2014年、中国のハッカーが、ERPシステムにゼロデイ脆弱性を利用したマルウェアを入れて米国物流会社に納品し、**企業会計や物流データを中国に裏で送っていた。**

2．海事分野でのサイバーインシデント事例②

- ✓ 黒海付近では、この2,3年間で**1万件ほどの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**が出ている。
- ✓ 2019年3月の米国シンクタンク（C4ADS)の発表では、これは**ロシアによるGPSスプーフィング行為が原因**であるという裏付けが示されている。





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

2．海事分野でのサイバーインシデント事例③

2017年 Maerskでランサムウェア感染により約330億円の損失

経緯：

- ✓ 2017年4月、ウクライナの会計アプリの更新サーバーがハッキングされ、ラトビアの偽サーバから、**新型ランサムウェア "NotPetya"に感染した更新ファイルがすり替わってダウンロードされていた**
- ✓ 2017年6月27日、ウクライナ黒海沿岸にあるオデッサのMaerskオフィスで、同アプリを更新し、**コンピュータが同ランサムウェア**に感染
- ✓ 同社**インフラ全体に広がり、約4000台のサーバ、4万5000台のPCに影響**
- ✓ 10日間にわたり多くの業務が停止。対応コストは**約330億円とも。**
  完全復旧には2カ月以上。**多くの顧客からの信頼性を失った**とされている。

※10日間で回復できたのは、停電していたガーナのサーバのおかげとも。

出典：https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

2．海事分野でのサイバーインシデント事例③

2017年 Maerskでランサムウェア感染により約330億円の損失

経緯：

✓ 2017年4月 アプリの更新サーバーがハッキングされ

これは、非標的型の攻撃で、Maersk 以外にも、FedEx（子会社のTNTで約33億円の損失）など、多くの企業が影響を受け、総被害額は約1300億円以上とも試算されている。

これは”対岸の火事”ではない

こういったサイバー攻撃を、完全に防御することは難しく、
攻撃されていることをいかに早期発見し、対応、回復するかという
“サイバーレジリエンスの向上”も重要となっている。

出典：https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

3.1. IMO、各国船級・機関のサイバーセキュリティ対応の動向

2017年6月のIMO MSC98の決議により、船主・運航者は、**2021年1月1日以降の最初の適合証書の年次検査までに、ISMコードに基づく安全管理システム（SMS）を通じてサイバーリスク管理を実施することが”推奨”**される事となった。

The Guidelines on Cyber Security onboard Ships - Version 3, **BIMCO** (Nov. 2018)

他分野におけるサイバーセキュリティのガイドライン等

- **NIST Framework and SP800 series** – computer security policies, procedures and guidelines
- **ISO 27001** – ISMS: Information Security Management System
- **IEC 62443** – Security for industrial automation and control systems

海事分野におけるサイバー関するガイドライン等

- **IMO, MSC (98)** – Cyber risk management onboard ships should be included in SMS as of 1 Jan 2021 (Jun 2017)
- **BIMCO** – The guidelines on Cyber Security onboard ships Ver.3
- **IACS** – UR-E22, 12 Recommendations
- **DNV-GL**– Recommended practice or notation of cyber security onboard ships (2016), Cyber Secure (Basic/Adv.)
- **ABS** – Cyber Safety Program
- **BV** – Rules on Cyber Security (NR659)
- **LR** – Ship Right

3.2.日本における海事サイバーセキュリティの議論と対応

✓ **（一財）日本船舶技術研究協会　(JSTRA)**
「海事分野におけるサイバーセキュリティ対策に関する調査研究委員会」
■期間：2016年度～2018年度（3カ年）
■主な取り組み
1）海事サイバーセキュリティに関する国際動向を調査・把握
2）船舶におけるサイバーリスク管理・アセスメント手法の調査
※DNV-GL、ABS船級と連携したワークショップの実施
3）具体的な対策として、**安全管理システム(SMS）マニュアルでのサイバーリスク管理SMSテンプレートを作成**
※ABS船級との連携。LR・DNV-GL・ClassNKのレビュー実施

⇒ **今後、各運航者は2021年1月に向け、SMSにサイバーリスク管理を含めていくことが求められてくるが、このSMSテンプレートが、船舶運航に関するサイバーリスク管理のレベル向上に貢献することが期待されている。**

✓ **（一財）日本海事協会（ClassNK）**
2018年度末に、船舶サイバーセキュリティに関するガイドラインを公表
さらにテュフラインランド(ドイツ)との連携で、2019年度から本格的に、
サイバーセキュリティに関する認証サービスの構築に取り組んでいる。

⇒サイバーリスクマネージメント(運航船)

マネジメントの視点
IT的要素が強い

主な既存規格：
ISO 27000 Series
NIST Framework

IMO MSC-FAL.1/Circ.3
ISM-Code改訂においてサイバーリスクマネージメントの記載を推奨（2021年1月以降）
OCIMF, TMSA 3-13

各船級 管理系ガイドライン・認証
- **LR**…Cybersecurity Maturity Framework
- **DNV-GL**…RP:CyberSecurity Resilience Management、Cyber secure (Basic)
- **BV** …CYBER MANAGED
- **ClassNK** … マネジメントガイドライン

BIMCO, ICS, InterTanko (BIMCO guideline) Ver.3
→Annex B: SMS Template

規格化
ISO TC8/SC1/WG6

既存の国際標準・規格

JSTRAのSMSテンプレート

海事分野への適用の流れ

主な既存規格：
IEC 62443 Series
NIST SP800

IACS …
- UR-E22
- 12 Recommendations

各船級 設計・建造系ガイドライン・認証
- **ABS** … CYBERSAFETY CS/ CS Ready
- **LR** … ShipRight
- **BV** … SYS-COM、CYBER SECURE
- **DNV-GL** …Cyber secure (Advanced)
- **ClassNK**…システムデザインガイドライン

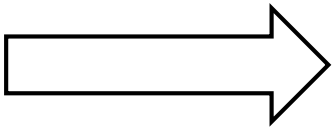
規格化
IEC61162-460 (航海計器ネットワーク)
ISO16425 (船内LAN)

物理的な制御・監視の視点
OT的要素が強い

⇒ サイバーレジリアント船(新造船)

3.3. 新造船と就航船における対応

建造中



就航後

サイバーリスクマネジメントの継続的な運用とレベル向上

サイバーレジリエント船の建造

サイバーレジリエンスの継続的な保守とレベル向上

造船所がシステムインテグレータ

船主・運航者がシステムインテグレータ

⇒ システムインテグレータを中心として、
様々なプレーヤーが互いに協力・連携していくことが必要

- 船主／運航者／管理会社
- 造船所／サプライヤー
- 船級協会
- 衛星通信会社　・・・

4. NYKグループにおけるこれまでの取り組み

✓ 2016～2018年度

- JSTRA 海事サイバーセキュリティ検討委員会への参加と調査
- SMSにおける**サイバーリスクマネジメントの対応準備**

✓ 2018年度

- 運航船において、**船級によるサイバーリスクアセスメント**を実施し、**現状のリスクマネジメントレベルと脆弱性を把握**

✓ 2019年度

- 運航船の**サイバーリスクマネジメントレベル向上のため、各船級と連携し、**
  - ➢ サイバーセキュリティ対策ワークショップの実施
  - ➢ eラーニング、**教育プログラム**の作成　etc.
- 船舶機器の**脆弱性テストのトライアル(計画中)**

サイバーレジリエンスの継続的な保守とレベル向上

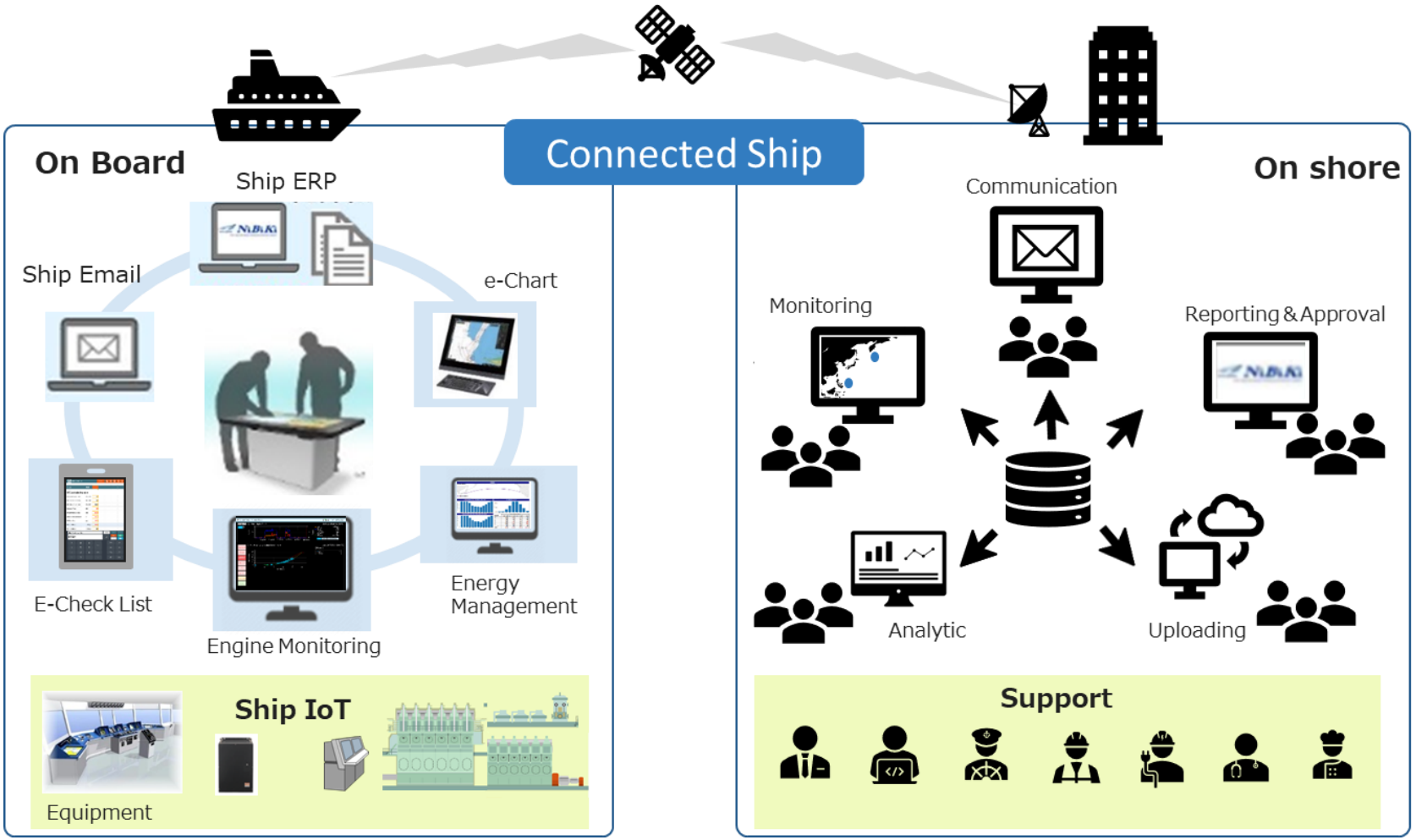
サイバーリスクマネジメントの継続的な運用とレベル向上

4. NYKグループにおけるこれからの取り組み①

対象となるフェーズ	新造船の計画・建造	就航船のオペレーション
キーコンセプト	**Security by Design**	**Security Management**
関係する既存規格・認証等	➢ IACS UR-E22 / 12 Recommendation ➢ 各船級 機器・OT系ガイドライン・認証 ・ ClassNK：システムデザインガイドライン ・ ABS CYBERSAFETY CS/ CS Ready 等	➢ IMO MSC-FAL.1./Circ.3 ➢ 各船級や組織のガイドライン ➢ JSTRA委員会作成 SMSテンプレート
現在の課題等	1. ガイドラインはあるが具体的な対応内容はまだ不明確。 2. 実運用上、システムインテグレータや機器メーカ、サプライヤーにどこまでの対応・準備が求められるのかが明らかでない。	1. JSTRA作成SMSテンプレートなどを参考に、船舶運航者・管理者は、自社のSMSをサイバー対応を盛り込んでいく。 2. SMSの内容を基にしたトレーニングの実施など、運用・改善体制を構築していく。
今後の対応 **赤枠**：運航者の対応 **青枠**：JSTRA, JSMEA (スマナビ研3) での対応	**【JSTRA】船舶サイバーレジリエンス向上に向けた調査研究** （上記の課題１に対応） ↓ 連携・情報共有 **【JSMEA/スマナビ研3】サイバーセキュリティ検討WG** （上記の課題１、２に対応） フィードバック **船舶機器サイバー脆弱性テスト**	**SMSにおけるサイバーセキュリティ対応プランの作成** （上記の課題１に対応） ↓ 実運用への落とし込み **オペレーション・運用体制の構築・教育プログラム作成** （上記の課題２に対応）

4. NYKグループにおけるこれからの取り組み②

船陸データ通信を活用した、”Connected Ship”が今後ますます広がっていく



4. NYKグループにおけるこれからの取り組み②

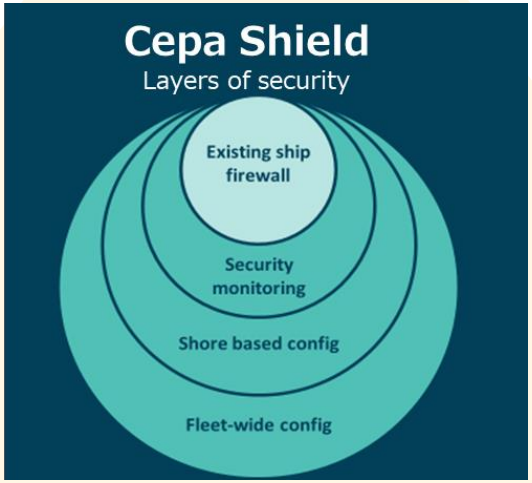
NYK LINE NIPPON YUSEN KAISHA

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)

5. これから求められるサイバーセキュリティ対応①

＜船主・運航者＞

- ✓就航船では、**SMSにおけるサイバーリスクマネジメント対応**が必要
- ✓攻撃者は、**2021年1月まで待ってくれない**
  →対応プランや社内外と連携した体制の構築は**急務**
- ✓リスクマネジメントにおいては、船と陸も含めたすべての関係者に定期的なサイバーセキュリティ**Awareness・トレーニングも重要**
- ✓サイバーレジリエンス向上の観点では、
  就航後は、**船主・運航者がシステムインテグレータ**となって、
  造船所・サプライヤー・船級等と連携して運用およびサイバーレジリエンスレベルの継続的な維持と向上が必要

5. これから求められるサイバーセキュリティ対応②

＜造船所＞

- ✓新造船では、**造船所がシステムインテグレータ**として中心となり Security by Designの視点で、**サプライヤーや船主・船級等と協力連携**し、サイバーレジリエント船への対応が必要
- ✓就航後のリスクマネジメントのレベルを向上させるために、**建造段階から、先を見越した準備と対応**が必要
  - e.g. 船内OT/ITネットワークトポロジー図、サイバー対応FMEA など
- ✓**各船級のサイバーシステム認証**に対応できるような事前準備が必要

＜サプライヤー＞

- ✓**機器自体のサイバーレジリエンス向上対応も**求められてくる
  - e.g. 定期的なAdminパスワードの変更、未使用ポートのブロック など
- ✓どのような対応が求められるか今のうちから準備が必要
- ✓今後、**船舶の高度自動化や自律船**の議論・実装が進むと、ますますサプライヤーのサイバーレジリエンス向上対応が重要

ご清聴ありがとうございました