2.　サイバーセキュリティについて

～ その重要性，業界の動きとNKの取組み ～

1.　サイバーセキュリティ

1.1　はじめに

コンピュータ技術の進化は目覚ましく，インターネット，電子メール，スマートフォンなど身近なものだけを見ても，ほんの数年前と比較して明らかに判るほど急速な発展を遂げている。また，そのような技術は今や日常生活に欠かせないものになっているといっても過言ではない。

しかし，コンピュータ技術の発展は便利さをもたらす一方で，副産物のようにサイバーリスクを伴っている。このことを，頭では理解していても，どこか他人事のように思って真剣に対策をとっていないということはないだろうか。対策をとっていてもサイバー攻撃を完全に防ぐことはほぼ不可能といわれる中，対策をとっていない又はそれが不十分であれば，ある日突然，想像を超えた大きな損失を被ることになる可能性が懸念される。

サイバー攻撃には，注意して探さなければ気が付かないような目立たないものもあり，現時点ではその危険性に対する認識に大きな個人差があるかもしれない。しかし，平穏だと思っていても一寸先は闇だという危機意識を持って適切に対処することが極めて重要である。また，組織のセキュリティレベルを考えた場合，部門間にレベルの差があると，その中でセキュリティレベルが最も低い部門がセキュリティ防御の突破口になりうるため，すべての関係者がサイバーセキュリティを適切に認識すべきである。このことは，陸上でも船上でも共通することであり，サイバーセキュリティは海事業界全体にとっても避けて通れないものになっている。

本稿では，サイバーセキュリティとは何かという点に立ち戻り，そこから業界やIMOの動きをたどってその重要性や方向性を確認し，また，NKの取組みについて紹介する。

1.2　ウイルスの感染経路

まず手始めに，身近なところで，コンピュータ・ウイルスの感染経路について見てみる。ここに例示するものは，その一部にすぎないが，これを見るだけでもウイルス感染の手口が巧妙化しており，うっかりするとコンピュータをウイルスに感染させてしまいかねないことを再認識できるであろう。

インターネットに接続していないコンピュータであっても，USBメモリ等の記憶媒体を介してウイルスに感染することがある。多くのコンピュータでは，USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されており，この仕組みを悪用して，コンピュータに感染するウイルスがある。このようなウイルスの中には，感染したコンピュータに後から差し込まれた別のUSBメモリに感染するなどの方法で，

被害を拡大させるものもある。

電子メールの添付ファイルもウイルスの感染経路として一般的である。電子メールに添付されてきたファイルをよく確認せずに開くと，それが悪意のあるプログラムであった場合はウイルスに感染してしまう。かつては，電子メールで実行形式のファイル（ファイルの拡張子が.exe のファイル）が送られていたときは特に注意するようにいわれていたが，最近はファイル名を巧妙に偽装し，文書形式のファイルに見せかけて悪意のあるプログラムを実行させ，ウイルスに感染させる事例もある。また，文書形式のファイルであっても，文書を閲覧するソフトウェアの脆弱性を狙った攻撃も増加していることから，メールに添付されてきたファイルを安易に開くのは危険な行為である。

インターネットを利用する際に用いられる Web ブラウザは，ホームページ上で様々な処理を実現できるように，各種のプログラムを実行できるようになっている。これらのプログラムの脆弱性を悪用するウイルスが埋め込まれたホームページを閲覧すると，それだけでコンピュータがウイルスに感染してしまう危険がある。かつては怪しい Web サイトを訪問しなければ大丈夫と思われていたが，最近では正規の Web サイトが不正侵入を受けて書き換えられ，ウイルスが仕込まれてしまうケースも急増している。この場合は，正規の Web サイトを閲覧しても，ウイルスに感染してしまうことになる。

また，あたかも無料のウイルス対策ソフトのように見せかけて，悪意のあるプログラムをインストールさせようとする「偽セキュリティソフト」の被害が増えている。その代表的な手口は，ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し，利用者を偽のウイルス対策ソフトを配布する Web サイトに誘導する方法である。

1.3　攻撃目的の変化と，攻撃手法の巧妙化

旧来のサイバー攻撃は，自己顕示，見せしめ，嫌がらせ等を目的とした愉快犯によるものが多かった。しかし，最近では金銭等を目的とした経済犯・組織犯により行われる計画的で悪質なものが増加し，危険度が高まっている。

また，攻撃を受けた側がすぐにそれに気づいて対策を講じることが可能であるような目立つ攻撃に加えて，攻撃手法の巧妙化により目立たない攻撃が増加し，攻撃の発覚が遅れ，被害が拡大・長期化し，深刻化する傾向にある。

後述の BIMCO 等により作成された「船舶のサイバーセキュリティに関するガイドライン」（以下，「BIMCO ガイドライン」という。）においても，会社や会社が運航する船舶に対する脅威及びその結果が**表 1** のようにまとめられている。また，同ガイドラインでは，会社の陸上及び船上の従業員がサイバーシステム及びデータを損傷することもあり得るとし，一般的にはそれが意図的ではなく，IT システム及び OT システムの運用や管理のミス，あるいは技術的及び手続的な防御手順の遵守違反で生じることを考慮して準備すべきであるとしつつも，不満を抱いた従業員が会社及び船舶に損害を与えるために悪意を持って故意に行う可能性もあることを指摘している。

表 1　動機と目的

グループ	動機	目的
活動家 （不満を抱く従業員を含む）	・名誉棄損 ・業務妨害	・データの破壊 ・機密データの暴露 ・メディアの注目 ・標的のサービスやシステムへのアクセス妨害
犯罪者	・金銭目的 ・商業スパイ ・産業スパイ	・盗んだデータの売却 ・盗んだデータの身代金要求 ・システム操作の身代金要求 ・不正な貨物輸送の手配 ・より巧妙な犯罪，貨物の正確な位置，船外の輸送及び取扱計画等に関する機密情報収集
日和見主義者	・挑戦	・サイバーセキュリティ防御の突破 ・金銭目的
国家 国家に支援される組織 テロリスト	・政治目的	・情報収集 ・経済及び重要な国家インフラの妨害

（出典: 船舶のサイバーセキュリティに関するガイドライン（BIMCO 他））

2.　今，船舶に対策が必要か？

2.1　船舶を取り巻くコンピュータ技術の革新とそれに付随するサイバーリスク

近年，船舶を取り巻くコンピュータ技術においても革新が進んでいる。その結果として得られている又は得られつつあるプラスの要素として，例えば次に掲げるようなものが挙げられる。

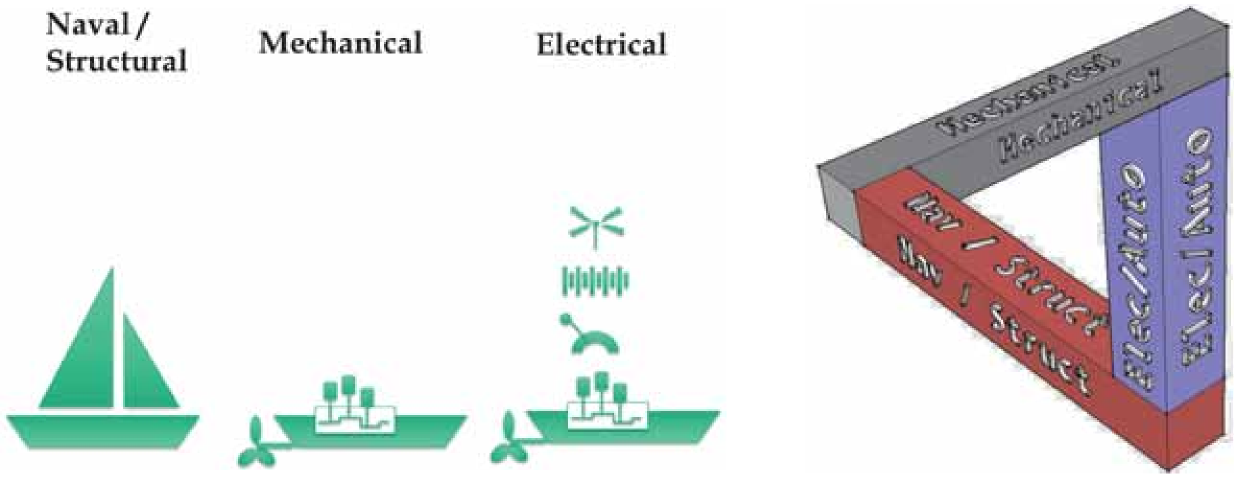
- 陸上施設との通信頻度，通信容量の増加
- インターネットや携帯端末等の利用機会の増加
- 船内機器のネットワーク化
- IoT 有効活用（最適航路の算出，機器の状態監視等）

しかしその一方で，これらのコンピュータ技術の革新による恩恵を享受しながら，サイバーセキュリティの防御を怠ると，悪意を持つ者が船内のシステムにアクセスするリスク等のマイナスの要素が付随するということを忘れてはならない。

有用なコンピュータ技術とサイバーリスクは表裏一体であり，有用なコンピュータ技術の進歩と共に，サイバーリスクも発展する。このため，万全なサイバーリスク対策は，コンピュータ技術の放棄を除いて，ほぼ不可能であるといえる。従って，現実的には，サイバーリスクを管理して上手に付き合っていく必要があり，そのためには船内のシステムのみならずそれを用いる人の認識も重要である。言い換えると，サイバーセキュリティ防御の突破口になってしまわないよう，すべての関係者がサイバーセキュリティの重要性を認識すべきである。

2.2　最近の船舶におけるサイバーセキュリティの重要性

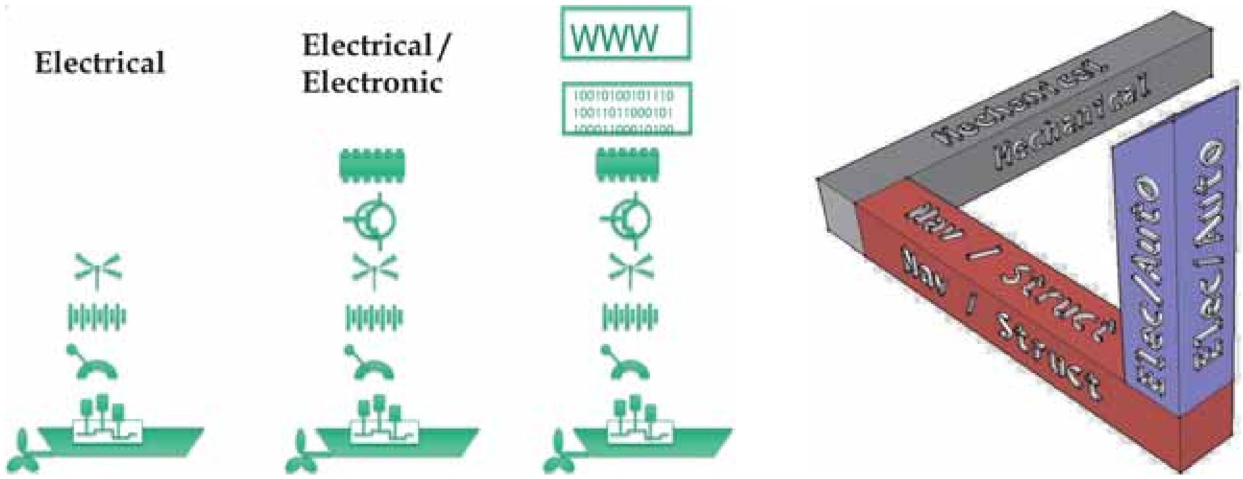
しかし，これまで長年にわたってサイバーセキュリティ上の問題なく運航されてきた船舶を見てきた方々の中には，今，船舶にサイバーセキュリティを求められることについて得心がいかない方もいらっしゃるのではないだろうか。そこで，最近の船舶におけるサイバーセキュリティの重要性を紹介した資料を以下に示す。当該資料は，IACS の取組みを紹介するために，2017 年 6 月に開催された IMO 第 98 回海上安全委員会において IACS により行われたプレゼンテーション資料の一部である。



(a)　(b)

図 1　Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security（その 1）

(1) 船舶の原理的な部分は，古典的なものに始まり，今日にも引き継がれている。そこへ導入された複雑な機械は天候への依存を減らし，電気は安全性を向上させた（図 **1-(a)**）。これまで，海事業界の人々は，既存の知識と経験をバランスよく活用してきた（図 **1-(b)**）。一方で，新たに開発されたものの利点も，それほど深く理解せずに活用していた。



(a)　(b)

図 2　Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security（その 2）

(2) エレクトロニクスによる複雑な制御技術は，操作者の技能を補助及び／又は代行した。当該技術は機能していても目に見えず，広く理解されないまま利用され，また，そこに移行された技能の重要性に見合った注意も払われなかった。結果的に，独立したシステムを繋ぐ機能は更なる利益をもたらしたが，既に理解が失われた部分については，エレクトロニクスによる制御技術への依存を高め，それをさらに複雑にした（図 **2-(a)**）。
そして，そこにはギャップがあるということを頭では理解していても，関係者の多くは，その重大さを十分に認識できなかった。目の錯覚のように，現実が納得して受入れられなかった（図 **2-(b)**，右上に隙間がある）。

(3) 海事業界としては，できることならば，サイバーの問題が起こらずに済んで欲しい。バランスの取れた居心地のよい頃に戻りたい（図 **1-(b)**，少し異なる視点から図 **2-(b)**の対象物を見てもこれと同様に見える）。

(4) この問題を理解し，対処するためには，古い考えを捨てて現実を受け入れる必要がある。見かけ上の「ギャップ」は，小さくないし空虚でもない（図 **3**，異なる角度から図 **2-(b)**の対象物を見たもの）。

(5) そこには，航海設備，データ収集，保護装置，通信プロトコル，ドライバ，機器制御，インターネット接続等，様々なものが存在している（図 **4**，更に回転させて図 **2-(b)**の対象物を見たもの）。

(6) そこには「システムの知識」も含まれており，他の工学分野と同様に理解して取扱われるべき複雑な工学が何層にも重なって詰まっている（図 **5**）。

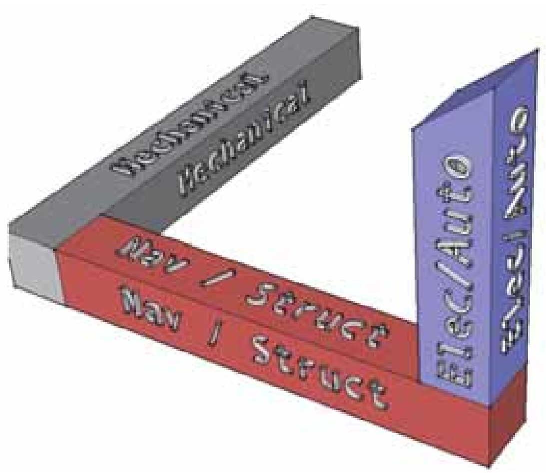


図 3　Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security（その 3）

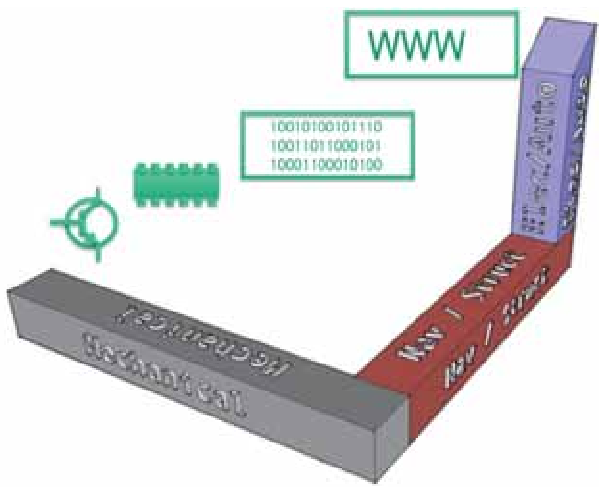


図 4　Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security（その 4）

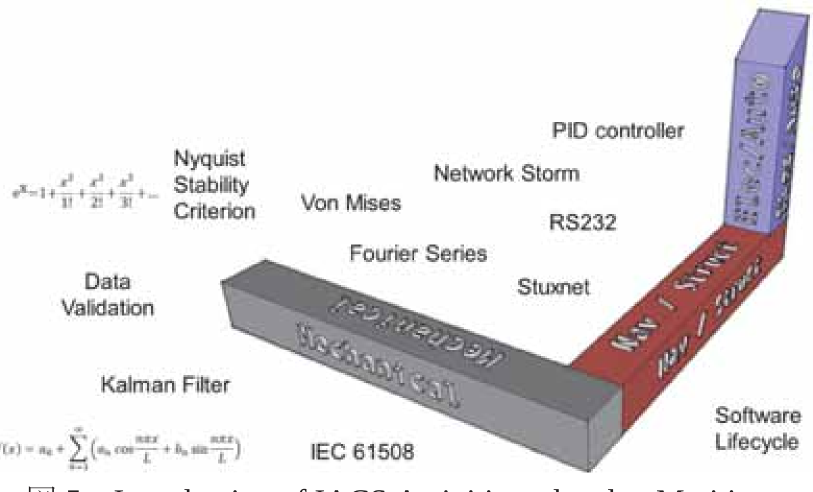


図 5　Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security（その 5）

2.3　サイバー攻撃

BIMCO ガイドラインにおいて，サイバー・インシデント及びサイバー攻撃は，次のように定義されている。

サイバー・インシデント：船内システム，ネットワーク及びコンピュータ又はそれらにより処理，保管もしくは送信される情報に，悪影響をもたらす又はもたらしうる出来事。その影響を抑えるために対応措置が必要な場合がある。

サイバー攻撃：IT システム，OT システム（船内システムを監視及び管理する装置，センサ，ソフトウェア，関連するネットワーク等），コンピュータ・ネットワーク及び／又はパソコンを標的として，企業や船内のシステムやデータを危険にさらし，破壊し又はアクセスしようとするあらゆる種類の攻撃的行為。

そして，陸上では，例えば英国全域でサイバー攻撃により病院のコンピュータに障害が発生し，予約や治療が不能になるといった，人命にかかわるサイバー攻撃があったとの報告もある。また，海事業界でも，「あなたの船は恐らく既にサイバー攻撃を受けている」あるいは「海運へのサイバー攻撃は予想よりも広く蔓延している」などという話もある。

海事業界では，以下に示すようなサイバー攻撃が発生したとされる又は発生しうるという情報もある。ただし，サイバー攻撃であるのか単なる故障や人的ミスであるのかについて見分けることは難しい。ここに挙げたものもあくまでも例であり，サイバー攻撃であると誰もが認めるものではないし，事実でない空想も含まれている。しかし，サイバー攻撃は日々巧妙化しており，いつその被害に遭っても不思議ではない。サイバー攻撃にはこのような性質があることからも，適切に対策を立てることが重要である。

・E メールに示された代金振込先の銀行口座や請求額が改ざんされていることに気づかずに送金したため，代金を詐取された。
・ECDIS に表示される電子海図が改ざんされていたため，あるいは GPS 信号の妨害により表示される船位が実際の船位と異なっていたため，衝突や座礁の危険にさらされた。また，当該 ECDIS 又は GPS の不具合に対処するために航行に遅延が生じた。さらに，故意に衝突させることが可能になればテロ行為につながることも考えられなくはない。
・コンテナヤードのシステムに対するサイバー攻撃により，荷役が不可能になるようにプログラムが不正に操作され，業務が妨害された。
・浮体式石油プラットフォームに対するサイバー攻撃により，プラットフォームの傾きが制御できなくなり，かつ，その原因究明と復旧に何日もかかり，その間，操業停止に追い込まれた。
・港湾のシステムに不正に侵入され，違法な薬物が積載されたコンテナを探し出した上当該コンテナを運び出して奪われた後，そのような行為が明るみに出ないよう関連する記録も削除された。
・海運会社のシステムに不正に侵入して各船舶における保安体制と積荷を特定し，高価な積荷を積載している割に保安体制が甘い船を探し出した海賊が，当該積荷を容易に強奪した。

3.　業界の動き

3.1　ISO規格（「製品」に対する認証）

情報技術セキュリティの観点から，情報技術に関連した製品及びシステムが適切に設計され，その設計が正しく実装されていることを評価するための基準として，ISO 15408 情報セキュリティ技術の評価基準があり，これを用いて約 30 製品に対する認証が実施されている。しかし，これらの製品は，一番大きなものでも「デジタル複合機」にとどまっている。このような状況下で，船舶へのサイバーセキュリティは，マネジメントからのアプローチが主流となっている。

3.2　ISO 規格（マネジメントからのアプローチ）

船舶のサイバーセキュリティに特化したものではないが，次に掲げる ISO 規格が広く用いられている。

・ISO 27001 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項

（情報の機密性・完全性・可用性をバランスよく管理し，情報を有効活用するための組織の枠組が示されている。）

・ISO 27002 情報技術 - セキュリティ技術 - 情報セキュリティ管理策の実践のための規範

（ISO 27001 の附属書 A に示される情報セキュリティ管理策の導入する上で役に立つ具体的な実施方法が示されている。）

3.3　NIST フレームワーク

米国の安全保障を危険に晒す重要インフラのサイバーリスクへの対策強化に関する大統領令（2013 年 2 月）を受け，業界標準及びベストプラクティスをまとめ，企業におけるサイバーリスクの低減及びより適切な管理を支援することを目的として，米国国立標準技術研究所（NIST: National Institute of Standards and Technology）より，「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」の初版が 2014 年 2 月に発行され，2018 年 4 月にはその第 1.1 版が発行されている。

その冒頭の記載によると，本フレームワークは，企業に新たな規制を課すことなく，ビジネスニーズに基づいてコスト効率よくサイバーセキュリティリスクに対処し，そうしたリスクを管理するための「共通言語」を記しているとのことである。

3.4　BIMCO ガイドライン

船主及び運航会社が船舶のサイバーシステムのセキュリティを維持できるように，サイバーセキュリティの運用評価方法及び必要な手順と措置の実行方法を提示することを目的として，国際的な海運組織である BIMCO，CLIA，ICS，INTERCARGO 及び INTERTANKO より，「船舶のサイバーセキュリティに関するガイドライン」の初版が 2016 年 1 月に発行され，2017 年 7 月にはその第 2 版が発行されている。また，2019 年初頭には第 3 版が発行

される見込みである。なお，本ガイドラインの作成においては，上述の NIST フレームワークも使用されている。

4. IMOの動き

2017 年 6 月に開催された第 98 回海上安全委員会において，非強制の MSC-FAL.1/Circ.3「海事分野のサイバーリスクマネジメントに関するガイドライン」が承認された。これは，2016 年 5 月に開催された第 96 回海上安全委員会において MSC.1/Circ.1526 として承認されていたものが改めて MSC（海上安全委員会）及び FAL（簡易化委員会）の合同のガイドラインとして承認されたものである。内容は，背景，適用，サイバーリスクマネジメントの要素に加えて，サイバーリスクマネジメント実行のためのベストプラクティスとして，BIMCO ガイドライン，ISO 27001，NIST フレームワークを紹介するものである。

また，同じ第 98 回海上安全委員会において，非強制の決議 MSC.428(98)「安全管理システムにおける海事分野のサイバーリスクマネジメント」が採択された。その内容は，サイバーリスクマネジメントは ISM コードに従って安全管理システムにおいて考慮されるべきであることを確認し, 2021 年 1 月 1 日より後, 最初に行われる ISM の会社年次審査までに，安全管理システムの中でサイバーリスクを取扱うことを奨励するものである。

IMO 加盟国も具体的に動きだしており，2018 年 6 月にはドイツ政府から，サイバーリスクマネジメントを会社の既存の安全管理システムに取入れる方法の一例を助言的に示すサーキュラーが発行されている。

5. IACS及びNKの取組み

5.1 IACS Recommendation

IACS では 2016 年 7 月に Cyber Systems Panel を新たに設置した。当該 Panel では現在，船主，造船所，無線業者，旗国等の代表者から構成される Joint Working Group の協力を得て，サイバーシステムに関する次の 12 の Recommendation を作成中である。

1. ソフトウェア保守手順
2. 機器の手動/機側制御
3. 緊急時対応計画
4. ネットワーク構造
5. データの保証
6. 物理的セキュリティ
7. ネットワークセキュリティ
8. 船舶システムデザイン
9. システムの一覧
10. インテグレーション
11. 遠隔アップデート/アクセス
12. 通信及びインターフェース

これらは，船上の IT システム及び OT システムのハードウェア及びソフトウェアに関して推奨される事項をまとめるものであり，それぞれの関係は，**図 6** に示すように，全体の考え方を示すもの，堅牢な設計を実現するためのもの，システムの回復力に貢献するものの大きく 3 つに分けられる。また，これらの統合版の作成に向けた検討も開始される予定である。なお，これらの具体的な内容は，本稿執筆時にはまだ公表されていないが，近日中に IACS のウェブサイトに公表されることが見込まれている。

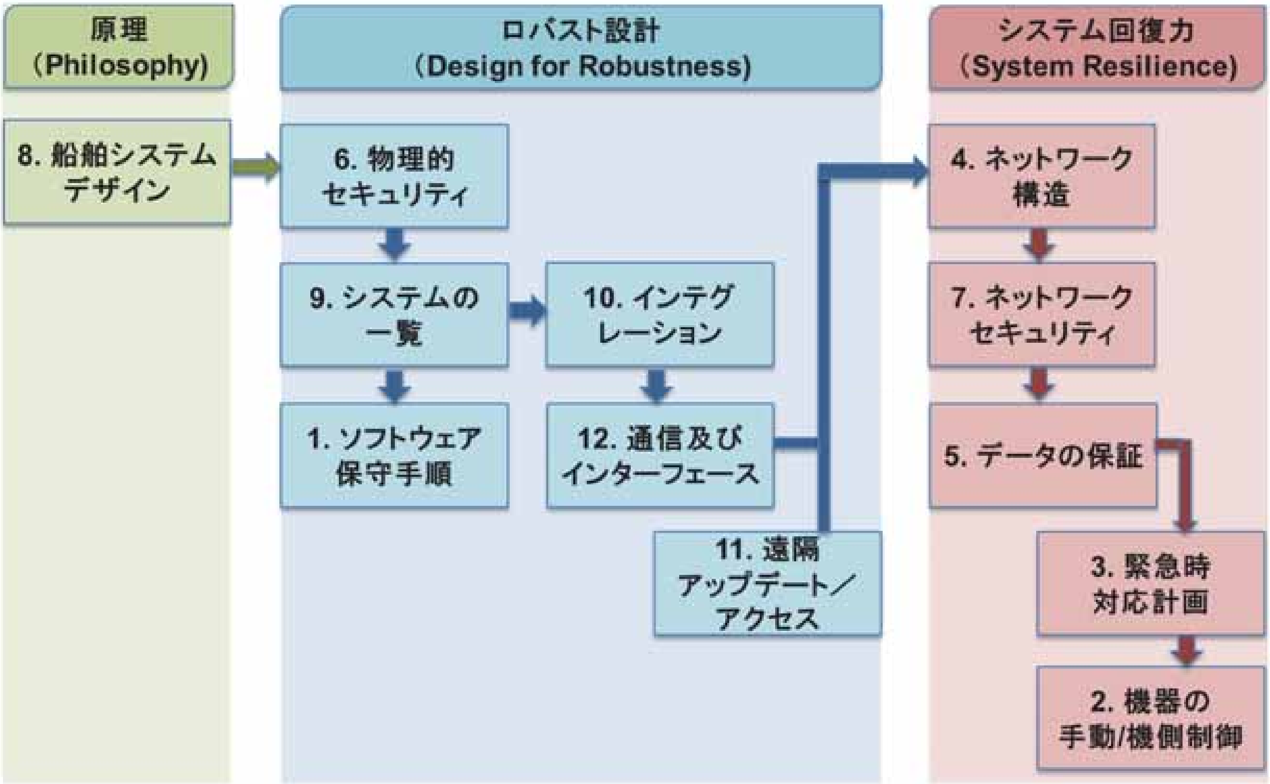


図 6　IACS で作成中の 12 の Recommendation の関係

5.2　　NK の取組み

(1)　IACS Recommendation を基にしたガイドラインの作成

本会も，IACS メンバーとして，上述の IACS Recommendation の作成に参画している。また，何をすることが求められているのかという情報を業界に提供することを目指して，IACS Recommendation を基に，必要な事項を加えたガイドラインの作成準備を進めている。

(2)　サイバーセキュリティマネジメントシステム（CSMS）の認証

3.1 で述べたとおり，船舶へのサイバーセキュリティはマネジメントからのアプローチが主流となっているため，マネジメントの認証に向けて準備を進めている。

以下に示すリスクマネジメントの基本原則のうち，(a)に記載されているリスクの特定の例としては，船内の主要システム（例えば，ブリッジシステム，通信システム，船内事務室，荷役制御システム，機関制御及び推進システム，アクセスコントロールシステム，バラスト水管理システム，安全システム，警報制御システム等）を資産として捉え，「サイバー攻撃対策が不十分（脆弱性）なブリッジシステム（資産）に，サービス妨害攻撃（脅威）がなされることにより，船舶の運航に支障をきたし，荷主への遅延・損害が生じる（結果）」とすることなどが考えられる。

＜リスクマネジメントの基本原則＞

(a) リスクの特定
- 守るべき資産と脅威，脆弱性の洗い出し
- 起こりうる結果の特定

(b) リスク分析
- 結果の影響度，起こりやすさ等からリスクレベルを分析
- 受容可能な基準を設定し，分析結果と比較

(c) リスク対応策の決定
- 「リスク低減」リスク対策をとる
- 「リスク回避」リスクのある活動を行わない
- 「リスク共有」リスクを他者と共有する（保険を掛けるなど）
- 「リスク保有」何も対策を取らない

(3) 船上に搭載される各種ソフトウェアシステムの認証

ソフトウェア開発のプロセスに対する既存のサイバーセキュリティの規格を参考にして，認証に向けて準備を進めている。

6. まとめ

近年ではサイバー攻撃の目的が変化しており，従来の愉快犯に加えて経済犯や組織犯が増えてきたことに伴い，攻撃の手法が巧妙化し，被害に遭う危険度が高まっている。

船舶においても，有用なコンピュータ技術の進歩の恩恵が受けられるようになる一方，それと表裏一体で発展するサイバーリスクを管理することが求められるようになっている。サイバー攻撃は日々巧妙化しており，いつその被害に遭っても不思議ではないということを念頭において，サイバーセキュリティ防御の突破口になってしまわないよう，すべての関係者がサイバーセキュリティの重要性を認識すべきである。

船舶のサイバーセキュリティは，マネジメントからのアプローチが主流であり，BIMCO ガイドライン，ISO 27001，NIST フレームワーク等が参考になる。

IMO では，2021 年 1 月 1 日より後，最初に行われる ISM の会社年次審査までに安全管理システムにてサイバーリスクが適切に取扱われることを奨励している。また，一部の旗国からは関連するサーキュラーが発行されており，今後，強制要件が示されることも考えられるので，旗国からの情報に注意が必要である。一方 IACS では，海事業界の協力を得て Recommendation を作成中である。参考までに，IMO の動きと関連業界の動きをまとめたものを**図 7** に示す。

本会でも，当該 Recommendation を基にしたガイドラインの作成，サイバーセキュリティマネジメントシステム（CSMS）の認証及び船上に搭載される各種ソフトウェアシステムの認証を準備中である。今後も，日々状況が変わっていく中で，専門の関係機関とも連携しつつ情報を収集して，業界への情報提供に努めていく所存である。

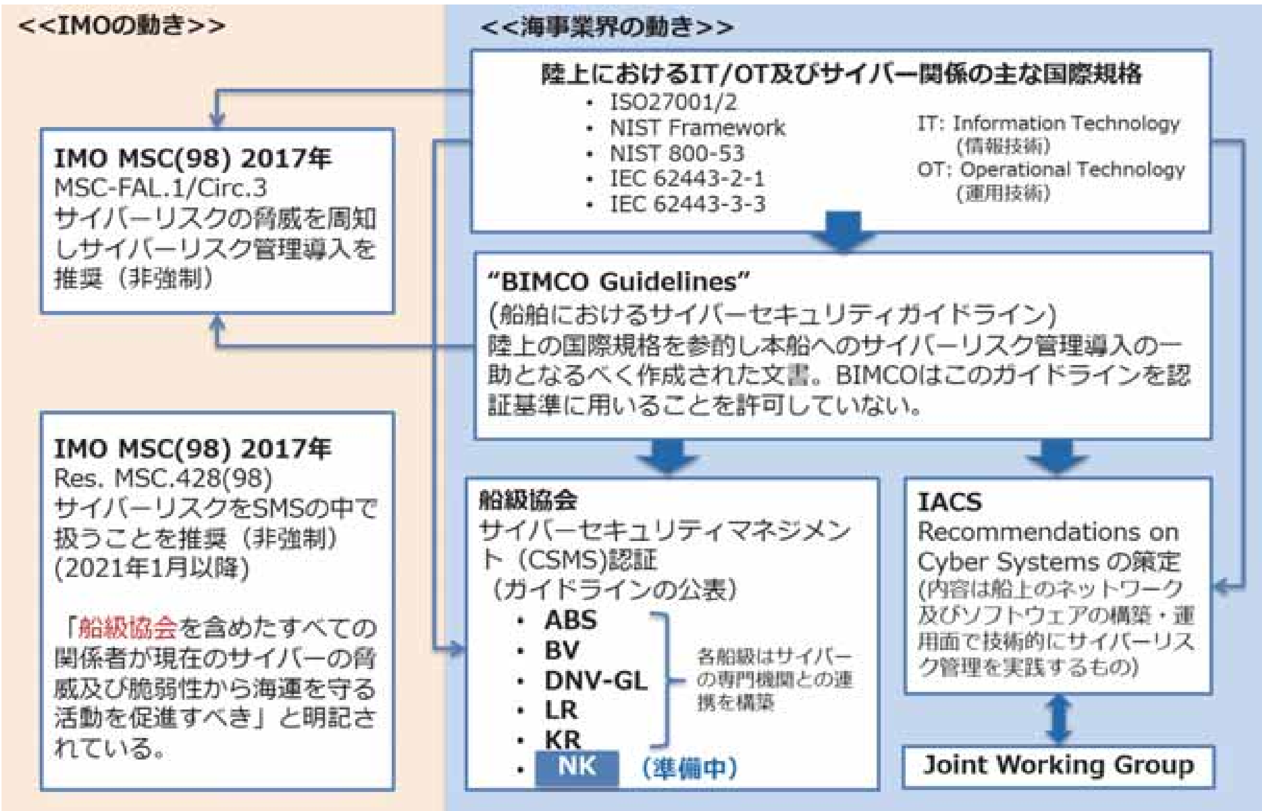


図 7　IMO の動きと海事業界の動き

2018 ClassNK秋季技術セミナー ClassNK

サイバーセキュリティについて

～その重要性，業界の動きとNKの取組み～

1

目　次 ClassNK

1. サイバーセキュリティ
2. 今，船舶に対策が必要か？
3. 業界の動き
4. IMOの動き
5. IACS及びNKの取組み

2

サイバーセキュリティ　ClassNK

・コンピュータ技術の発展

インターネット，電子メール，スマートフォン，・・・

・サイバーリスク

他人事？ある日突然・・・

・組織のセキュリティレベル

最もレベルの低い部門が，セキュリティ防護の突破口に

サイバーセキュリティは，海事業界全体で
すべての関係者が避けては通れない。

3

サイバーセキュリティ　ClassNK

身近なコンピュータ・ウイルスの感染経路の例

・USBメモリ
・電子メールの添付ファイル
・ホームページの閲覧
  ・ウイルスが埋め込まれたホームページを閲覧するだけでコンピュータがウイルスに感染してしまう危険がある。
  ・最近では正規のWebサイトが不正侵入を受けて書き換えられウイルスが仕込まれてしまうケースも急増している。この場合怪しいWebサイトではない正規のWebサイトを閲覧してもウイルスに感染してしまうことになる。
・信頼できないサイトで配布されたプログラムのインストール

（総務省『国民のための情報セキュリティサイト』（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/02-1.html）を加工して作成）

4

サイバーセキュリティ

ClassNK

愉快犯　：　自己顕示，見せしめ，嫌がらせ等が目的

攻撃目的が変化，
攻撃手法が巧妙化し
危険度が高まる

経済犯
組織犯　：　金銭等が目的 ⇒ 計画的，悪質

サイバーセキュリティ

ClassNK

グループ	動機	目的
活動家 （不満を抱く従業員を含む）	・名誉棄損 ・業務妨害	・データの破壊 ・機密データの暴露 ・メディアの注目 ・標的のサービスやシステムへのアクセス妨害
犯罪者	・金銭目的 ・商業スパイ ・産業スパイ	・盗んだデータの売却 ・盗んだデータの身代金要求 ・システム操作の身代金要求 ・不正な貨物輸送の手配 ・より巧妙な犯罪，貨物の正確な位置，船外の輸送及び取扱計画等に関する機密情報収集
日和見主義者	・挑戦	・サイバーセキュリティ防御の突破 ・金銭目的
国家 国家に支援される組織 テロリスト	・政治目的	・情報収集 ・経済及び重要な国家インフラの妨害

（出典：船舶のサイバーセキュリティに関するガイドライン（BIMCO他））

目　次

ClassNK

7

今，船舶に対策が必要か？

ClassNK

船舶を取り巻くコンピュータ技術の革新 （プラス要素）

・陸上施設との通信頻度，通信容量の増加
・インターネットや携帯端末等の利用機会の増加
・船内機器のネットワーク化
・IoT有効活用の試み（最適航路の算出，機器の状態監視等）

⇕

付随するサイバーリスク （マイナス要素）

・コンピュータ技術の革新による恩恵を享受
⇒サイバーセキュリティの防御を怠ると
⇒悪意を持つ者が船内のシステムにアクセスするリスク

8

今，船舶に対策が必要か？ ClassNK

有用なコンピュータ技術とサイバーリスクは表裏一体。つまり，
有用なコンピュータ技術の進歩と共にサイバーリスクも発展する。

↓

万全なサイバーリスク対策は，ほぼ不可能。
（唯一確実な対策はコンピュータ技術の放棄）

↓

サイバーリスクを管理して，上手に付き合うことが必要。
船内のシステムのみならず，それを用いる**人の認識**も重要。

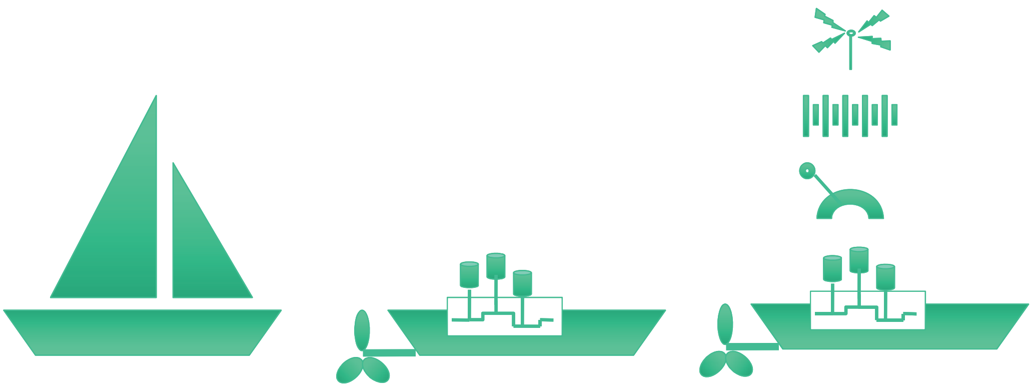
↓

サイバーセキュリティ防御の突破口になってしまわないよう，
すべての関係者がサイバーセキュリティの重要性を認識すべき。

9

今，船舶に対策が必要か？ ClassNK

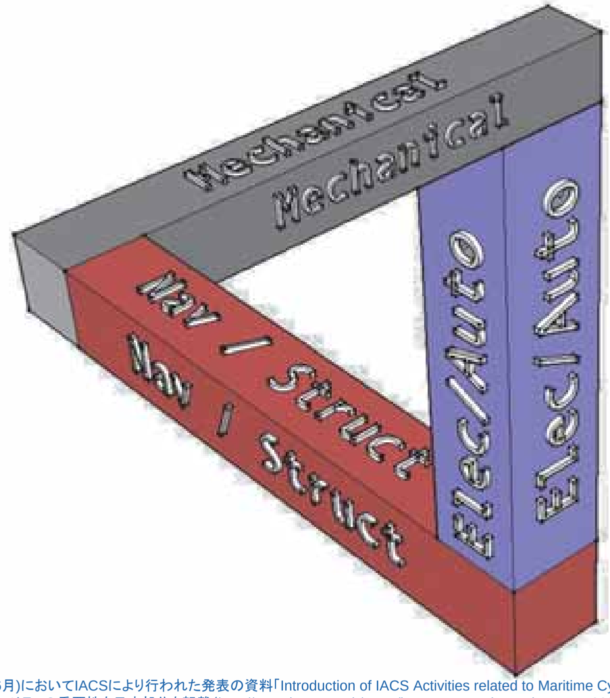
Naval / Structural | **Mechanical** | **Electrical**



IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

10

今，船舶に対策が必要か？



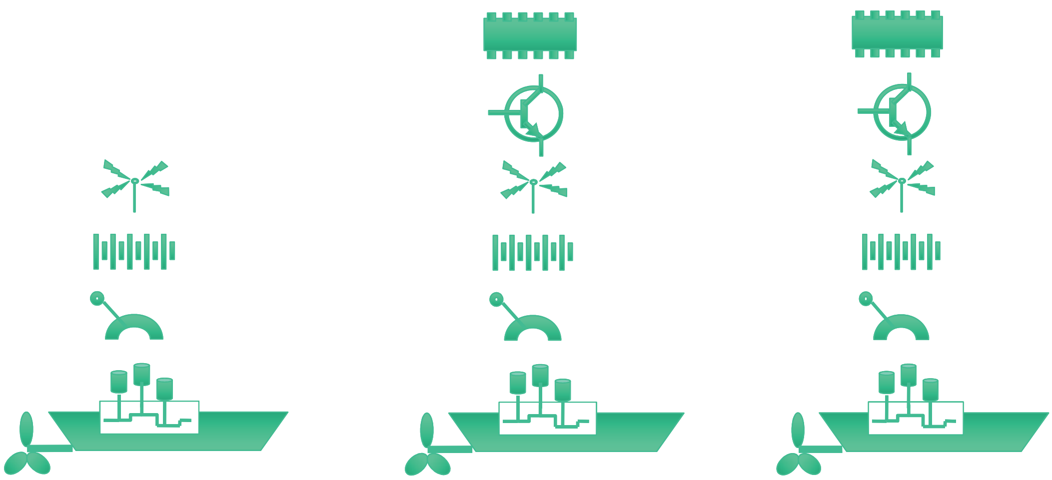
IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

11

今，船舶に対策が必要か？

Electrical

Electrical / Electronic



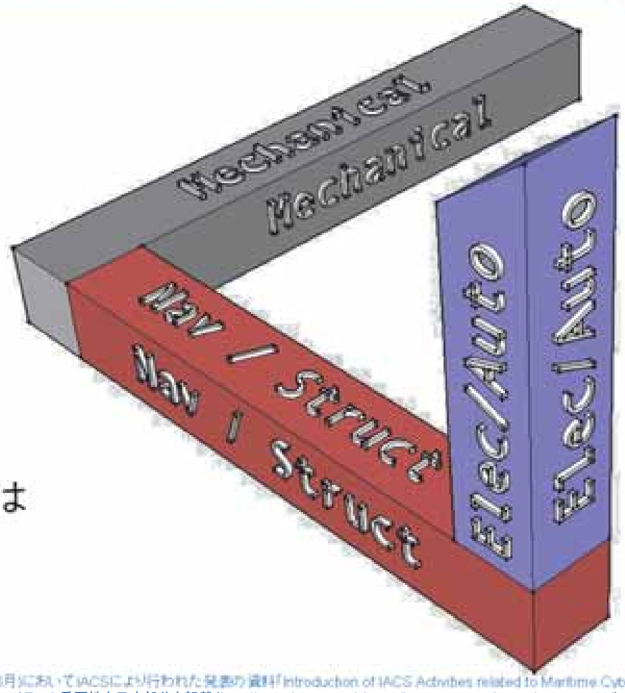
IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

12

今，船舶に対策が必要か？

ClassNK

過去5年や10年の間に
導入されたものは，
目でよく見えない。



海事業界の人々は，
造船学，構造，
機関に関する
重要なことについては
よく理解している。

IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

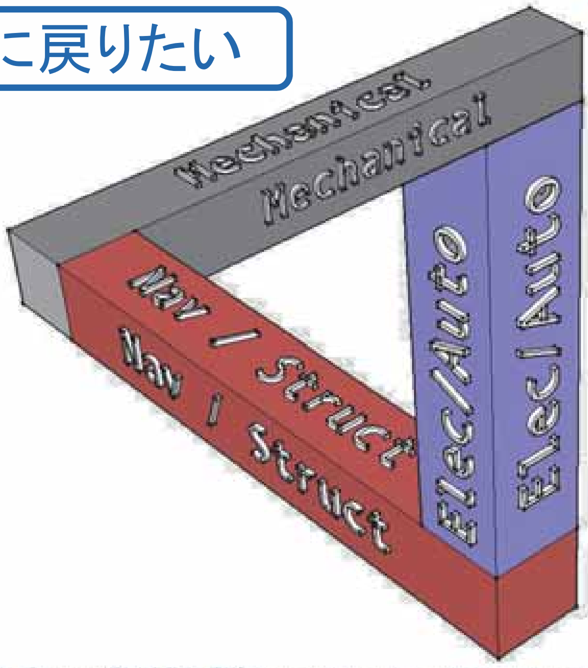
13

今，船舶に対策が必要か？

ClassNK

居心地のよい頃に戻りたい

海事業界としては，
できれば，サイバーの
問題が起こらずに
済んで欲しい。



IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

14

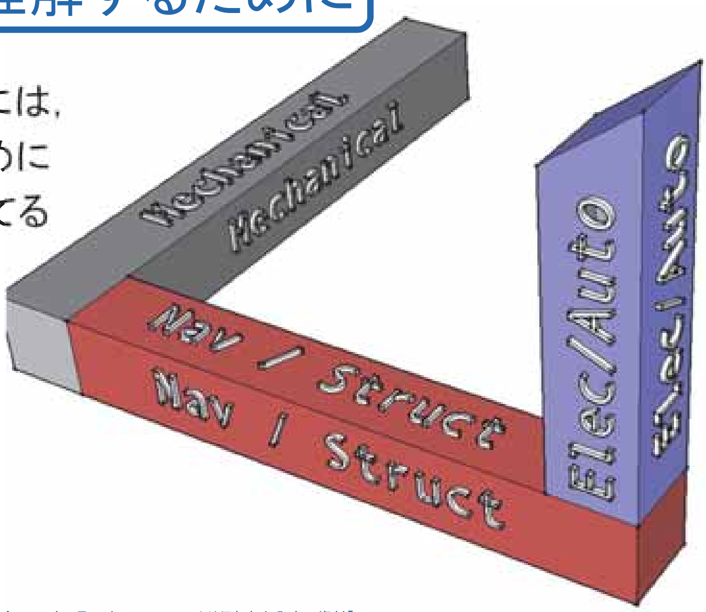
今，船舶に対策が必要か？

ClassNK

問題をもっと理解するために

この問題に対処するには，
現実を受け入れるために
皆が古い考え方を捨てる
必要がある。

見かけ上の
「ギャップ」は
小さくないし
空虚でもない・・・



IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

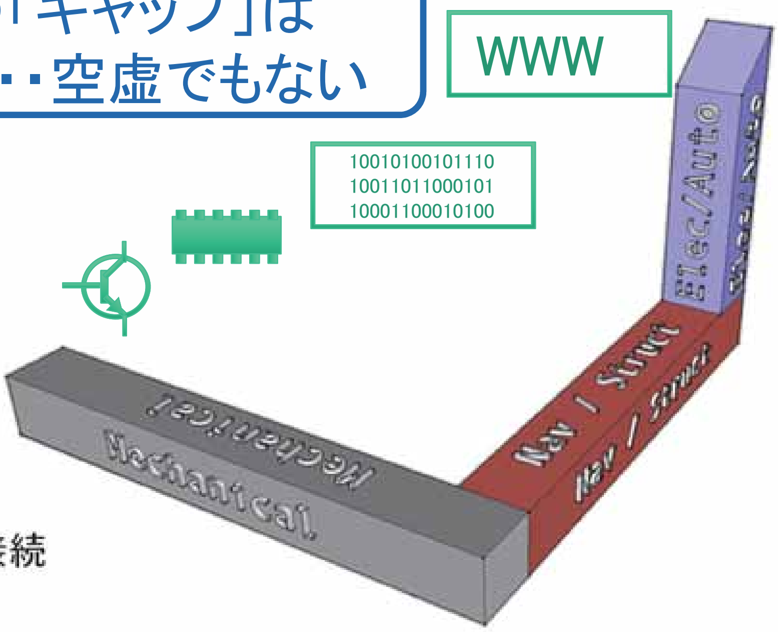
15

今，船舶に対策が必要か？

ClassNK

見かけ上の「ギャップ」は小さくない・・・空虚でもない

そこにあるのは，
- 航行援助装置
- データ収集
- 保護装置
- 通信プロトコル
- ドライバ
- 機器制御
- インターネット接続



IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

16

今，船舶に対策が必要か？

ClassNK

そこには「システムの知識」も含まれる

そこには「システムの知識」も含まれており，
他の工学分野と同様に理解して取扱われるべき
複雑な工学が何層にも重なって詰まっている。

PID controller

$e^{x}=1+\frac{x^2}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}+\dots$

Nyquist
Stability
Criterion

Network Storm

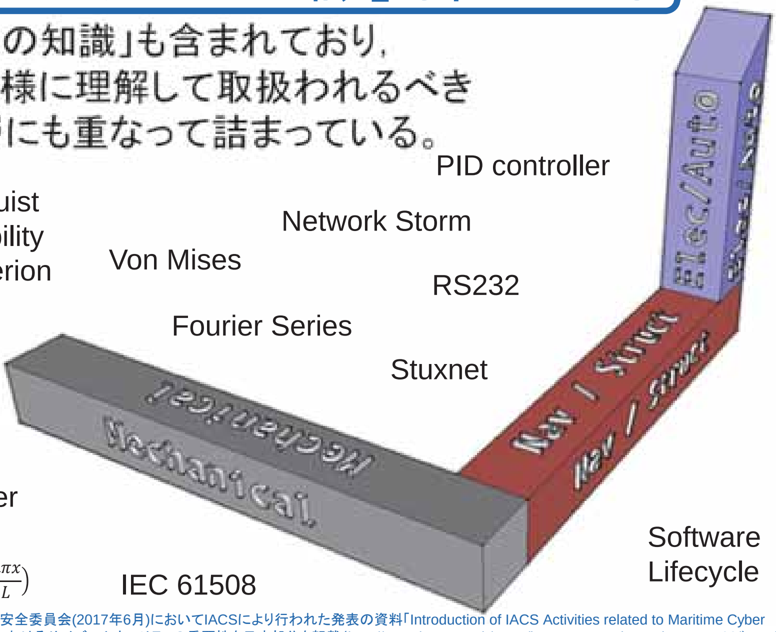
Von Mises

RS232

Fourier Series

Data
Validation

Stuxnet



Kalman Filter

Software
Lifecycle

$$f(x)=a_0+\sum_{n=1}^{\infty}\left(a_n\cos\frac{n\pi x}{L}+b_n\sin\frac{n\pi x}{L}\right)$$

IEC 61508

IACSの取組みを紹介するため，IMO第98回海上安全委員会(2017年6月)においてIACSにより行われた発表の資料「Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security」より，最近の船舶におけるサイバーセキュリティの重要性を示す部分を転載（http://www.iacs.org.uk/news/iacs-presentation-at-imo-msc-98/）

17

今，船舶に対策が必要か？

ClassNK

サイバー・インシデント

船内システム，ネットワーク及びコンピュータ又はそれらにより処理，保管もしくは送信される情報に，悪影響をもたらす又はもたらしうる出来事。その影響を抑えるために対応措置が必要な場合がある。

サイバー攻撃

IT及びOTシステム，コンピュータ・ネットワーク及び/又はパソコンを標的として，会社や船内のシステムやデータを危険にさらし，破壊し又はアクセスしようとするあらゆる種類の攻撃的行為。

OT (Operational Technology)

船内システムを監視及び管理する装置，センサ，ソフトウェア，関連するネットワーク等。

（出典：船舶のサイバーセキュリティに関するガイドライン（BIMCO他））

18

今，船舶に対策が必要か？ ClassNK

例えば…

≡ TIME | World

UNITED KINGDOM

「英国の病院，サイバー攻撃とみられる
大規模なコンピュータ被害発生」

Jill Lawless / AP
Updated: May 13, 2017 3:32 PM ET

「英国全域でサイバー攻撃により病院のコンピュータに障害が発生，
予約不能，回線がダウンし，治療不能に」

「あなたの船は恐らく既にサイバー攻撃を受けている」

March 31, 2017 by Editorial (Source: “gCaptain”)

「海運へのサイバー攻撃は予想よりも広く蔓延している」

Tue 21 Jun 2016 by Martyn Wingrove (Source: “Marine Electronics & Communications”)

19

今，船舶に対策が必要か？ ClassNK

海事業界で発生したとされる/発生しうるサイバー攻撃の例

- Eメールに示された送金先や請求額の改ざん ⇒ 送金を詐取
- ECDISの海図の改ざん，GPS信号の妨害による船位の改ざん
  ⇒ 衝突や座礁の危険，対応に伴う航行の遅延，テロへの悪用
- コンテナヤードのシステムへの侵入により荷役を不能に ⇒ 妨害
- 浮体式石油プラットフォームの傾きの制御を不能に ⇒ 妨害
- 港湾のシステムから，違法薬物を含むコンテナを探知 ⇒ 奪取
- 海運会社のシステムから，船舶の保安体制と積荷を特定
  ⇒ 海賊が高価な積荷を容易に強奪

サイバー攻撃であるのか，単なる故障や人的ミスであるのかについては，見分けることが難しい。ここに挙げたものもあくまでも例であり，サイバー攻撃であると誰もが認めるものではないし，事実でない空想も含まれている。しかし，サイバー攻撃は，日々巧妙化しており，いつその被害に遭っても不思議ではない。

20

目　次

ClassNK

21

業界の動き

ClassNK

陸　上

ISO規格（「製品」に対する認証）

ISO 15408　情報セキュリティ技術の評価基準

概要：情報技術セキュリティの観点から，情報技術に関連した製品及びシステムが適切に設計され，その設計が正しく実装されていることを評価するための基準
- 約30製品に対して認証を実施。
- 一番大きなものは「デジタル複合機」。

船舶へのサイバーセキュリティは，
マネジメントからのアプローチが主流

22

業界の動き

ClassNK

陸　上

マネジメントアプローチ

ISO規格（マネジメントからのアプローチ）

ISO 27001　情報技術 - セキュリティ技術 -
情報セキュリティマネジメントシステム - 要求事項

概要：情報の機密性・完全性・可用性をバランスよく管理して，
情報を有効活用するための組織の枠組が示されている。

ISO 27002　情報技術 - セキュリティ技術 -
情報セキュリティ管理策の実践のための規範

概要：ISO 27001附属書Aに示された情報セキュリティ管理策を
導入する上で役立つ具体的な実施方法が示されている。

23

業界の動き

ClassNK

陸　上

マネジメントアプローチ

NIST（米国国立標準技術研究所）

「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」
(NIST: National Institute of Standards and Technology)
初版：　2014年2月

目的:

米国の安全保障を危険に晒す重要インフラの
サイバーリスクへの対策強化に関する大統領令
（2013年2月）を受け，業界標準及びベストプラクティスをまとめ，企業におけるサイバーリスクの低減及びより適切な管理を支援すること

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

注：NISTフレームワークのその後の状況

- 第1.1版：2018年4月

24

業界の動き

ClassNK

海事業界

マネジメントアプローチ

BIMCO（ボルチック国際海運協議会）

「船舶のサイバーセキュリティに関するガイドライン」
(BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO)

初版：　2016年1月

目的:

船主及び運航会社が船舶のサイバーシステムのセキュリティを維持できるように，サイバーセキュリティの運用評価方法及び必要な手順と措置の実行方法を提示すること

注：BIMCOガイドラインのその後の状況
- 第2版：2017年7月　（国際海上保険連合(IUMI)が参加）
- 2019年初頭に第3版を発行予定

25

業界の動き

ClassNK

海事業界

マネジメントアプローチ

船舶のサイバー・セキュリティに関するガイドライン
(BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO)

目　次

ClassNK

27

IMOの動き

ClassNK

マネジメントアプローチ

第98回海上安全委員会（2017年6月）

「海事分野のサイバーリスクマネジメントに関するガイドライン」

（非強制）(MSC-FAL.1/Circ.3)

注：第96回海上安全委員会（2016年5月）において承認されていたMSC.1/Circ.1526が，改めて
MSC（海上安全委員会）及びFAL（簡易化委員会）の合同のガイドラインとして承認された。

目次:

1. 序
2. 一般
   - 2.1 背景
   - 2.2 適用
3. サイバーリスクマネジメントの要素
4. サイバーリスクマネジメント実行のためのベストプラクティス
（BIMCOガイドライン，ISO 27001，NIST Frameworkを紹介）

28

IMOの動き

ClassNK

マネジメントアプローチ

第98回海上安全委員会（2017年6月）

「安全管理システムにおける海事分野のサイバーリスクマネジメント」（非強制）(Res. MSC.428(98))

要旨:

1. サイバーリスクマネジメントは，ISMコードに従って，安全管理システムにおいて考慮されるべき。
2. 2021年1月1日より後，最初に行われるISMの会社年次審査までに，安全管理システムにてサイバーリスクが適切に取扱われること。

29

IMOの動き

ClassNK

ISM Cyber Security（ドイツ，2018年6月1日）

サイバーリスクマネジメントを，会社の既存の安全管理システムに取入れる方法の一例を助言的に示す旗国サーキュラーを発行。

30

目　次

ClassNK

1. サイバーセキュリティ
2. 今，船舶に対策が必要か？
3. 業界の動き
4. IMOの動き
5. IACS及びNKの取組み

31

IACSの取組み

ClassNK

- サイバーシステムパネル（2016年7月～）
  - 議長: ABS
  - メンバー: 12 の船級協会
- サイバーシステム・ジョイントワーキンググループ（2016年11月～）
  - 議長: ABS
  - メンバー:
    - 船級協会（8）
    - 業界団体
（4：CIRM, EUROMOT, Inmarsat, World Shipping Council）
    - 船社，オペレーター団体
（5：BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO）
    - 造船団体（2：Active Shipbuilding Experts' Federation,
Community of Europe Shipbuilding Association）
    - 旗国当局（4：カナダ，韓国，シンガポール，米国）

32

IACSの取組み

ClassNK

■ **IACS Maritime Cyber Systems Recommendations**

12のテーマの “Recommendation” を作成中。
また，それらの統合版の作成に向けた検討を開始予定。

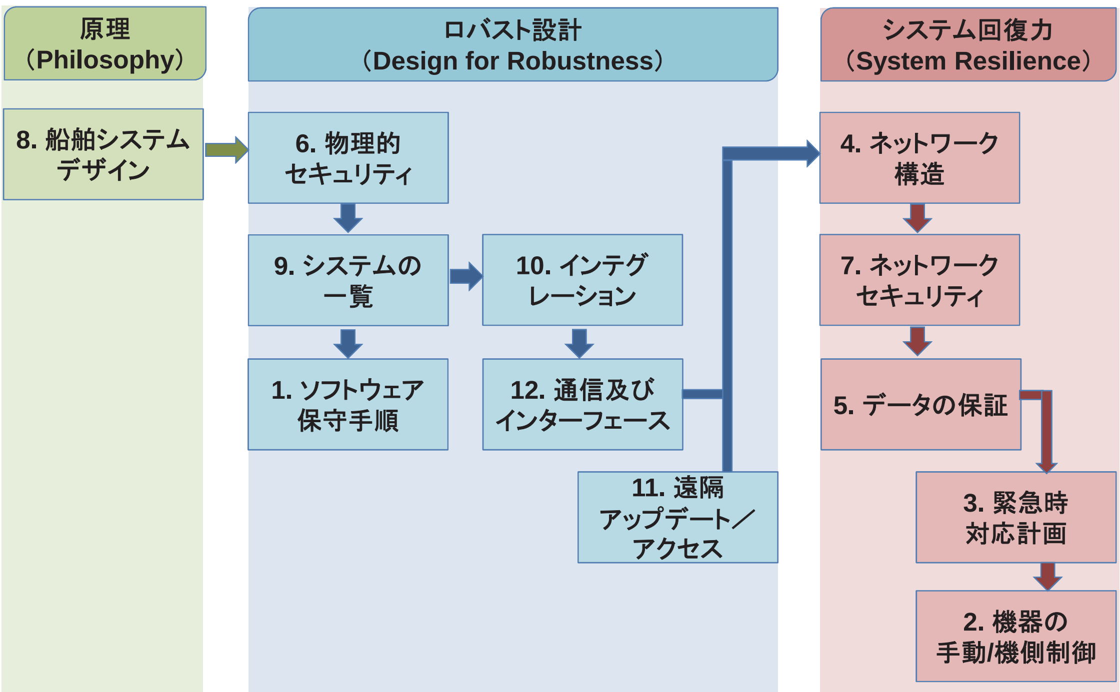
“IT/OTアプローチ”

1. ソフトウェア保守手順
2. 機器の手動/機側制御
3. 緊急時対応計画
4. ネットワーク構造
5. データの保証
6. 物理的セキュリティ
7. ネットワークセキュリティ
8. 船舶システムデザイン
9. システムの一覧
10. インテグレーション
11. 遠隔アップデート/アクセス
12. 通信及びインターフェース

33

IACSの取組み

ClassNK



34

NKの取組み

ClassNK

NKサイバーセキュリティサービスの構築へ向けて

① IACS Recommendationを基にしたガイドラインの作成

② サイバーセキュリティマネジメントシステム(CSMS)の認証

③ 船上に搭載される各種ソフトウェアシステムの認証

関係機関との連携を早期に構築

- IT・OT専門機関
- セキュリティ専門機関
- 研究機関

35

NKの取組み

ClassNK

<u>**リスクマネジメントの基本原則**</u>

1. リスクの特定

① 守るべき**資産**と**脅威**，**脆弱性**の洗い出し

② 起こりうる**結果**の特定

2. リスク分析

① **結果**の影響度，起こりやすさ等からリスクレベルを分析

② 受容可能な基準を設定し，分析結果と比較

3. リスク対応策の決定

① 「リスク低減」リスク対策をとる

② 「リスク回避」リスクのある活動を行わない

③ 「リスク共有」リスクを他者と共有する(保険を掛けるなど)

④ 「リスク保有」何も対策を取らない

36

NKの取組み

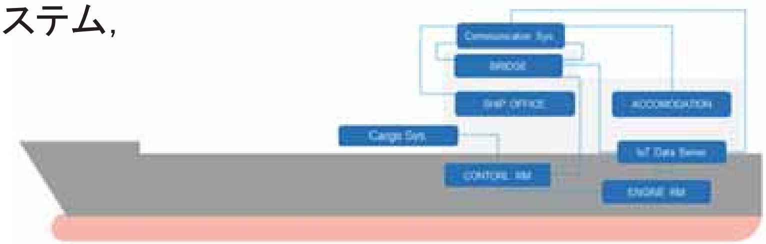
ClassNK

<u>船舶におけるサイバーセキュリティリスクの一例</u>

「サイバー攻撃対策が不十分(脆弱性)なブリッジシステム(資産)に，
サービス妨害攻撃(脅威)がなされることにより，船舶の運航に
支障をきたし，荷主への遅延・損害が生じる(結果)」

<u>アプローチ：船内の主要システムを「資産」として考える</u>

例)ブリッジシステム，通信システム，船内事務室，荷役制御システム，
機関制御及び推進システム，アクセスコントロールシステム，バラスト水
管理システム，安全システム，
警報制御システム



まとめ

ClassNK

- サイバー攻撃の目的が変化(愉快犯⇒経済犯・組織犯)，手法が巧妙化し，危険度が高まっている。

- 船舶においても，有用なコンピュータ技術の進歩と表裏一体で発展するサイバーリスクを管理することが求められる。サイバーセキュリティ防御の突破口になってしまわないよう，すべての関係者がサイバーセキュリティの重要性を認識すべき。

- サイバー攻撃は日々巧妙化しており，いつその被害に遭っても不思議ではない。

- 船舶のサイバーセキュリティは，マネジメントからのアプローチが主流。BIMCOガイドライン，ISO 27001，NISTフレームワーク等が参考になる。

まとめ

ClassNK

- IMOでは，2021年1月1日より後，最初に行われるISMの会社年次審査までに，安全管理システムにてサイバーリスクが適切に取扱われることを奨励。
- 一部の旗国から，関連するサーキュラー発行。今後，強制要件が示されることも考えられるので，旗国からの情報に注意。
- IACSでは，海事業界の協力を得てRecommendationsを作成中。
- NKでは，IACSのRecommendationsを基にしたガイドライン作成，サイバーセキュリティマネジメントシステム（CSMS）の認証及び船上に搭載される各種ソフトウェアシステムの認証を準備中。

39

まとめ

ClassNK

<<IMOの動き>>

IMO MSC(98) 2017年
MSC-FAL.1/Circ.3
サイバーリスクの脅威を周知しサイバーリスク管理導入を推奨（非強制）

IMO MSC(98) 2017年
Res. MSC.428(98)
サイバーリスクをSMSの中で扱うことを推奨（非強制）
(2021年1月以降)

「船級協会を含めたすべての関係者が現在のサイバーの脅威及び脆弱性から海運を守る活動を促進すべき」と明記されている。

<<海事業界の動き>>

陸上におけるIT/OT及びサイバー関係の主な国際規格
- ISO27001/2
- NIST Framework
- NIST 800-53
- IEC 62443-2-1
- IEC 62443-3-3

IT: Information Technology
(情報技術)
OT: Operational Technology
(運用技術)

“BIMCO Guidelines”
(船舶におけるサイバーセキュリティガイドライン)
陸上の国際規格を参酌し本船へのサイバーリスク管理導入の一助となるべく作成された文書。BIMCOはこのガイドラインを認証基準に用いることを許可していない。

船級協会
サイバーセキュリティマネジメント（CSMS)認証
（ガイドラインの公表）
- **ABS**
- **BV**
- **DNV-GL**
- **LR**
- **KR**
- **NK** **（準備中）**

各船級はサイバーの専門機関との連携を構築

IACS
Recommendations on Cyber Systems の策定
(内容は船上のネットワーク及びソフトウェアの構築・運用面で技術的にサイバーリスク管理を実践するもの)

Joint Working Group

40