February 2019

船舶におけるサイバーセキュリティマネジメントシステム

（要求事項及び管理策） [第 1 版]

[日本語/Japanese]

ClassNK サイバーセキュリティアプローチ

日本海事協会は，船舶のサイバーセキュリティに対する基本的な考え方について，国際機関や海事関連団体の動向も踏まえ，「ClassNK サイバーセキュリティアプローチ」をまとめました。

１．最重要事項は安全運航の確保

船舶におけるサイバーセキュリティ対策の重要な目的は安全運航の確保です。そのためには，船舶の運航を支える情報技術(Information Technology，IT)のみならず運用技術(Operation Technology，OT)における可用性の確保が優先すべき要素となります。

IT/OT 双方のサイバーリスク低減に向け，船舶及び船上機器類のセキュリティ・バイ・デザインな設計，就航中のマネジメントシステムの構築等，物理的，技術的，組織的アプローチをバランス良く組み合わせた対策を提案していきます。

２．サイバーセキュリティ対策の階層を設定

サイバーセキュリティ対策をいくつかの階層で整理の上，それぞれの階層ごとに，既存のサイバーセキュリティに関する国際規格等から船舶に適用可能と考えられる要件を採用し，「どの関係者が何をすべきか」について，明確に示していきます。

３．継続的な見直しと最新化

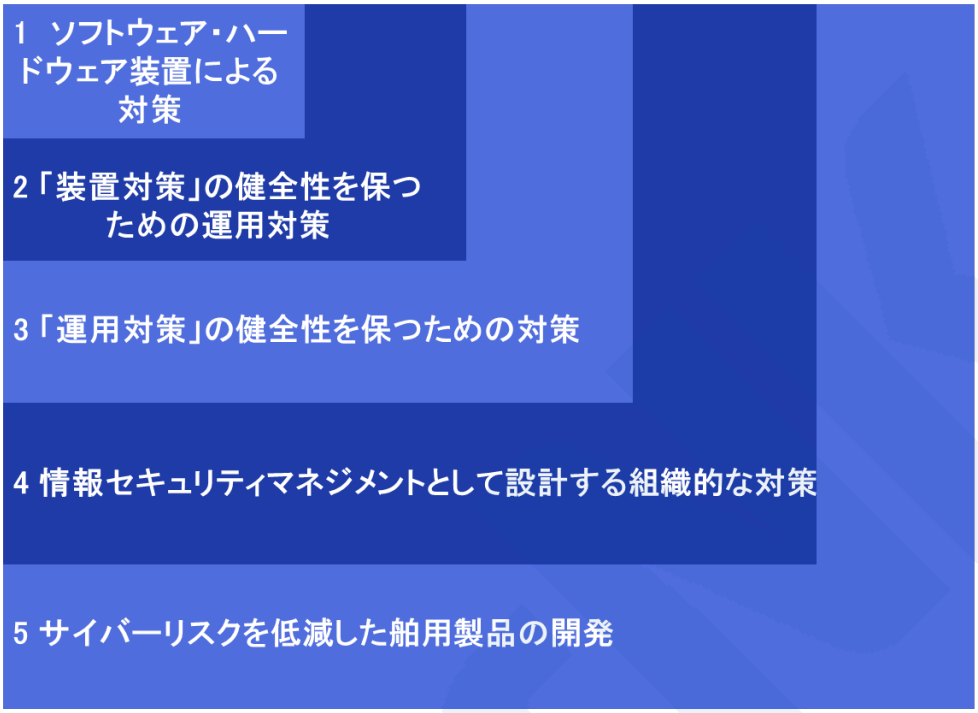
船舶運航における IT 化の進展やサイバーセキュリティの国際動向を踏まえ，最新の情報を専門家と共に分析し，船舶におけるサイバーセキュリティ対策について，その時点におけるベストプラクティスを提案していきます。

これらの考え方に基づき，サイバーセキュリティ対策の実施主体者と対策内容を示したガイドラインや規格を「ClassNK サイバーセキュリティシリーズ」として，随時公表していきます。

本ガイドラインの初版発行に際し，サイバーセキュリティに関する規格等を参考に，船舶において最低限必要と考えられる対策の抽出を試みました。しかしながら，実際に本ガイドラインに沿って講じられたサイバーセキュリティ対策は，不足又は過剰であることもありうると考えております。このため弊会では，本ガイドラインが船舶に対して最適なものとなるよう継続的に見直してまいります。

ClassNKサイバーセキュリティアプローチ

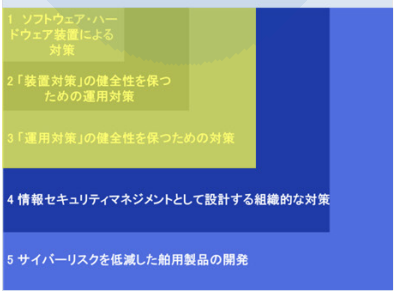
船舶のサイバーセキュリティ対策の階層



ClassNKサイバーセキュリティシリーズ

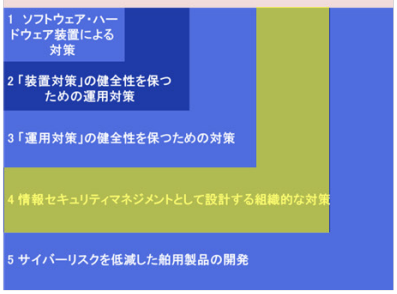
船舶における サイバーセキュリティ デザインガイドライン

- 対象：造船所及び建造船主
- NIST SP800-82を参考に，NIST SP800-53の中で船舶に適用できるものを抽出
- IACS Rec.の内容を精査



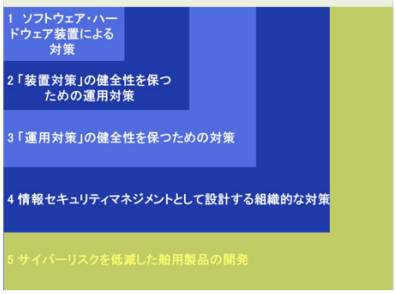
船舶における サイバーセキュリティ マネジメントシステム

- 対象：船舶管理会社及び船舶
- ISO27001及び27002の基本構造を参考にし，ISMコード体系との親和を図ったマネジメントシステム



ソフトウェアセキュリティ ガイドライン

- 対象：舶用機器メーカー
- ISO/IECの関係規格をベースに舶用に必要な要素を抽出したガイドラインに基づき，その開発プロセスと機能要件を検証する



改訂履歴

No.	日付	区分	改訂内容
1	2019.3.1	新規	新規作成

目次

序文		3
1	背景及び状況	3
2	定義	3
第1部	要求事項	5
1章	一般	5
1.1	目的	5
1.2	適用	5
1.3	サイバーセキュリティマネジメントシステム(CSMS)の機能的要件	5
2章	サイバーセキュリティ方針	6
2.1	サイバーセキュリティ方針の確立	6
2.2	サイバーセキュリティ方針の実施及び維持	6
3章	会社の責任及び権限	7
3.1	船舶の運航に責任を有する者の届け出	7
3.2	サイバーセキュリティ関連業務に係る責任の明確化	7
3.3	会社からの支援責任	7
4章	管理責任者	8
4.1	管理責任者の任命及び管理責任者の責任と権限	8
5章	船長の責任及び権限	9
5.1	船長の責任	9
5.2	船長の権限	9
6章	経営資源及び要員配置	10
6.1	船長の要件	10
6.2	配乗する人員の要件	10
6.3	教育	10
6.4	関係者の理解の確保	10
6.5	訓練	10
6.6	情報提供手順の確立	10
6.7	乗組員との意思疎通の確保	10
7章	船内業務	11
7.1	船内業務の確立	11
8章	緊急事態への準備	12
8.1	緊急事態への対応手順の確立	12
8.2	緊急事態への対応プログラムの確立	12
8.3	緊急事態への対応を確保する手段の提供	12
9章	不適合，事故及び危険発生の報告及び調査・解析	13
9.1	不適合，事故及び危険状態の報告	13
9.2	再発防止策	13
10章	船舶及び設備の保守	14
10.1	保守手順の確立	14
10.2	保守手順の要件	14
10.3	保守手順の継続性の確保	14
10.4	保守業務との関連性	14
11章	文書管理	15
11.1	文書管理手順の確立及び維持	15
11.2	文書管理手順の要件	15
11.3	サイバーセキュリティマネジメントマニュアル	15
12章	会社による検証，見直し及び評価	16
12.1	サイバーセキュリティマネジメントシステムの監査	16
12.2	供給者関係	16

12.3 サイバーセキュリティマネジメントシステムの評価 ・・・・・・・・・・・・・・・・・ 16
12.4 監査及び是正措置の実施 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 16
12.5 監査の独立性 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 16
12.6 レビュー結果の注意喚起 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 16
12.7 是正措置の実施 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 16
第 2 部 管理策 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 17
1 章 一般 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 17
1.1 目的 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 17
1.2 適用 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 17
1.3 サイバーセキュリティに係るリスクマネジメントと管理策の関係 ・・・・・・・・ 17
2 章 造船における管理策 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 19
2.1 サイバーセキュリティのための機能及び運用 ・・・・・・・・・・・・・・・・・・ 19
2.2 装置 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 20
2.3 情報通信機器 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 21
2.4 ネットワーク ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 22
2.5 情報 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 23
2.6 アクセス制御 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 24
2.7 物理的対策 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 26
2.8 緊急事態対応計画（コンティンジェンシー・プラン） ・・・・・・・・・・・・・・ 26
2.9 供給者関係 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 27
3 章 運航における会社の管理策・・・・・・・・・・・・・・・・・・・・・・・・・・・ 29
3.1 運航規則の整備 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 29
3.2 運航における支援及び管理・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 29
3.3 陸上の情報通信機器におけるセキュリティ対策 ・・・・・・・・・・・・・・・・・ 30
3.4 ログ取得及び監視・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 30
3.5 緊急事態対応 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 30
4 章 運航における船舶の管理策・・・・・・・・・・・・・・・・・・・・・・・・・・・ 32
4.1 装置・情報通信機器及びネットワークの管理・・・・・・・・・・・・・・・・・・・ 32
4.2 緊急事態対応 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 32
附属書 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 33
1 参考文献 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 33
2 海事分野における ICT 活用とサイバーリスク ・・・・・・・・・・・・・・・・・・ 34

序文

1　　背景及び状況

この「船舶におけるサイバーセキュリティマネジメントシステム」(NK-CSMS)は，会社及び船舶による，運航における船舶の安全確保を目的として，サイバーセキュリティに関するマネジメントシステムを確立し，実施し，維持し，継続的に改善するための活動の指針となるものである。NK-CSMS を会社及び船舶のプロセス及びマネジメント構造に組み込むことで，サイバーリスクを適切に評価し，管理することが期待される。また，NK-CSMS の適用に当たっては，本文書で示されるサイバーセキュリティ管理策のみならず，その組織のニーズ，目的，及び能力に応じることが望ましい。

この文書は以下の 2 部で構成する。

「第 1 部　要求事項」では，サイバーセキュリティマネジメントシステム (CSMS) の要求事項を定める。要求事項は，会社及び船舶に適用する。

「第 2 部　管理策」では，造船及び運航におけるサイバーセキュリティの管理策を定める。管理策は，会社及び船舶に実施する。

		対象	
		会社	船舶
第 1 部　要求事項		○	○
第 2 部　管理策	造船	○　2 章	―
	運航	○　3 章	○　4 章

2　　定義

以下の定義は，この文書の第 1 部及び第 2 部に適用する。

2.1　　サイバーセキュリティ

運航に係る装置，情報通信機器，ネットワーク及び情報を脅威から保護することによって，運航の安全を確保するとともに船上業務の適切な遂行を維持するために，会社及び船舶において行う活動をいう。

2.2　　会社

船舶所有者，又は船舶管理者もしくは裸用船者のようなその他の組織若しくは個人であって，船舶所有者から船舶の運航の責任を引受け，かつ，その引受けに際して，この NK-CSMS によって課されるすべての義務と責任を引き継ぐことに同意した者をいう。

2.3　　主管庁

船舶の旗国の政府をいう。

2.4　　サイバーセキュリティマネジメントシステム(CSMS)

会社の職員が会社のサイバーセキュリティの方針を効果的に実行できるように構築され，かつ，文書化されたマネジメントシステムをいう。

2.5　　サイバーセキュリティマネジメント証書

会社側及び船側での管理が，承認された CSMS に従って行われていることが明白である船舶に対して発行される文書をいう。

2.6　　客観的証拠

サイバーセキュリティ又は CSMS を構成する各要素そのもの及びその各要素の活動状況に関する，量的，質的な情報，記録及び事実の現認記述であり，それらは観察，測定及び試験に基づくもので，かつ検証が可能なものをいう。

2.7　　不適合

規定されている要求事項が満たされていないことを示す客観的証拠が観察された状況をいう。

2.8　　重大な不適合

人または船舶のサイバーセキュリティに重大な脅威，或いは環境に対し重大な危険を生じさせ，かつ直ちに是正措置を講じなければならないような明確な違反，もしくは CSMS の管理策が効果的に，かつ組織的に実行されていないことをいう。

2.9　　条約

1974 年の海上における人命の安全のための国際条約をいい，その後の改正を含む。

第 1 部 要求事項

1 章　一般

1.1　目的

1.1.1　一般

第 1 部の目的は，運航におけるサイバーセキュリティを確保することにある。

1.1.2　会社のサイバーセキュリティマネジメントの目的

会社のサイバーセキュリティマネジメントの目的として，特に次に留意しなければならない。

-1.　船舶運航時の安全な業務体制及び安全な作業環境の確保,

-2. その船舶, 人員及び環境について識別されたすべてのサイバーリスクの評価を行い適切な予防措置を確立すること，及び

-3.　サイバーセキュリティに関する緊急事態への準備を含めた, 陸上及び船上要員のサイバーセキュリティマネジメント技術の継続的改善。

1.1.3　関連する規則，条約，コード及び指針との両立性

CSMS は，次の事項を確保するものでなければならない。

-1.　適用される強制規則及び条約の遵守，及び

-2.　機関，主管庁，船級協会及びその他の海事関連団体が勧告する適用可能なコード，指針及び基準への配慮。

1.2　適用

第 2 部に定める管理策は，すべての船舶及び会社に適用することができる。

1.3　サイバーセキュリティマネジメントシステム(CSMS)の機能的要件

会社は，次の機能的要件を含む CSMS を構築し，実施し，維持しなければならない。

-1.　サイバーセキュリティの方針,

-2.　関連する条約及び旗国の法令に従い，船舶のサイバーセキュリティを確保するための指示書及び手順書,

-3.　陸上及び船内の組織内，及び組織間相互の権限の明確な位置付け及び情報伝達経路の明確な規定,

-4.　事故及び本要求事項の規定に対する不適合の報告手順書,

-5.　緊急事態に対する準備及び対応の手順書，及び

-6.　内部監査及び経営者による見直しに関する手順書。

2 章　サイバーセキュリティ方針

2.1　　サイバーセキュリティ方針の確立

会社は，**1.1** の目的を達成する方策を述べたサイバーセキュリティの方針を確立しなければならない。

2.2　　サイバーセキュリティ方針の実施及び維持

会社は，陸上及び船内の組織のすべての階層において方針が実施され，かつ，維持されることを確保しなければならない。

3 章　会社の責任及び権限

3.1　船舶の運航に責任を有する者の届け出

船舶の運航に責任を有する者が船舶所有者以外の場合，船舶所有者は，その船舶の運航に責任を有する者の名称等の詳細を主管庁に届け出なければならない。

3.2　サイバーセキュリティ関連業務に係る責任の明確化

会社は，サイバーセキュリティに関連する業務を管理，実行又は検証するすべての要員の責任，権限及び相互関係を明確にし，文書化しなければならない。

3.3　会社からの支援責任

会社は，管理責任者がその職務を果たすことが出来るように，適切な経営資源及び陸上からの支援の提供を確保する責任を有する。

4 章　管理責任者

4.1　　管理責任者の任命及び管理責任者の責任と権限

会社は，各船舶のサイバーセキュリティを確保し，かつ，会社と船舶との間の連携を図るため，経営責任者に直接接することができる管理責任者を任命しなければならない。管理責任者の責任と権限には，各船舶の運航に関しての サイバーセキュリティの状況を監視すること，並びに適切な経営資源及び陸上からの支援を，必要に応じて提供されることを確保とすることを含めなければならない。

5 章　船長の責任及び権限

5.1　　船長の責任

会社は，次に関する船長の責任を明確にし，文書化しなければならない。
-1. 会社のサイバーセキュリティ方針を実施すること，
-2. 乗組員が方針を遵守するよう動機付けること，
-3. 明確かつ簡潔な方法で，適切な命令及び指示を出すこと，
-4. 規定された要求事項が遵守されていることを検証すること，及び
-5. 定期的に CSMS の見直しを行い，かつ，その欠陥について経営者に報告すること。

5.2　　船長の権限

会社は，船舶で運用する CSMS の中に，船長の権限を強調した明確な記述が含まれること確保しなければならない。又，会社は，船長が，サイバーセキュリティに関する超越権限と，決定を下す責任を有し，かつ，必要に応じて会社の支援を要請できることを CSMS の中に確立しなければならない。

6 章　経営資源及び要員配置

6.1　船長の要件

会社は，船長が次の要件を満たすことを確保しなければならない。
-1. 船舶を指揮するための適切な資格を有していること，
-2. 会社の CSMS に十分精通していること，及び
-3. 職務を支障なく遂行できるように必要な支援を与えられていること。

6.2　配乗する人員の要件

会社は，各船舶に，
-1. 国内法及び国際法に従った免状，資格，及び身体適性を有する者を配乗していること及び
-2. 全ての局面での船上でのサイバーセキュリティ作業の維持を包含することができるよう適切に配乗していることを確保しなければならない。

6.3　教育

会社は，新たな要員及びサイバーセキュリティに関する職務に新たに配置転換された者が，その職務に対する適切な習熟訓練を受けられることを確保する手順を確立しなければならない。また，航海前に示されるべき重要な指示を識別し，文書化した上で出航前に乗組員に供与しなければならない。

6.4　関係者の理解の確保

会社は，会社の CSMS に関係する者全員が，関連する規則，条約，コード及び指針について十分な理解を有していることを確保しなければならない。

6.5　訓練

会社は，CSMS を擁護するために必要と思われる訓練を識別する手順を確立し， 維持しなければならない。また会社は，関係者全員にそのような訓練が与えられていることを確保しなければならない。

6.6　情報提供手順の確立

会社は，乗組員に，乗組員の使用言語又は理解できる言語で CSMS に関連する情報を提供する手順を確立しなければならない。

6.7　乗組員との意思疎通の確保

会社は，乗組員が CSMS に関連する職務を実行する場合に，効果的に意志疎通ができていることを確保しなければならない。

7 章　船内業務

7.1　船内業務の確立

会社は，人員と船舶のサイバーセキュリティに関する主要な船内業務に対し，必要に応じてチェックリストを含め，手順，計画及び指示を確立しなければならない。また，さまざまな責務を規定し，適切な資格を有する要員に割り当てなければならない。

8 章　緊急事態への準備

8.1　緊急事態への対応手順の確立

会社は，遭遇する可能性のある船舶の緊急事態を識別し，それらに対応するための手順を確立しなければならない。

8.2　緊急事態への対応プログラムの確立

会社は，緊急時の行動に備えるため，操練と演習のプログラムを確立しなければならない。

8.3　緊急事態への対応を確保する手段の提供

CSMS は，船舶が遭遇する危険，事故及び緊急事態に対し，会社の組織がいつでも対応し得ることを確保する手段を提供するものでなければならない。

9 章　不適合，事故及び危険発生の報告及び調査・解析

9.1　不適合，事故及び危険状態の報告

CSMS には，不適合，事故及び危険状態が会社に報告され，サイバーセキュリティの促進の目的に沿って調査及び解析されることを確保する手順が含まれていなければならない。

9.2　再発防止策

会社は，再発防止策を含めた是正措置実施のための手順を確立しなければならない。

10 章　船舶及び設備の保守

10.1　保守手順の確立

会社は，関連する規則・条約の規程及び会社で制定した追加の規程に従って船舶を保守することを確保する手順を確立しなければならない。

10.2　保守手順の要件

会社は，これらの要件を満たすために，次を確保しなければならない
-1. 点検が適正な間隔で実施されていること，
-2. すべての不適合は，もし判明していれば想定される原因とともに報告されていること，
-3. 適切な是正措置がとられていること，及び
-4. これらの実施記録を維持していること。

10.3　保守手順の継続性の確保

会社は，CSMS に突然作動が停止した場合に危険な状態を招くような設備及び機能を識別しなければならない。CSMS には，そのような設備又は機能の信頼性の向上を目的とした特別な手段を設けなければならない。この手段には，予備機器並びに連続して使用されない設備又は機能の定期的な試験を含めなければならない。

10.4　保守業務との関連性

10.2 の点検は，**10.3** の手段とともに，船舶が通常運航する際の保守業務に組込まれなければならない。

11 章　文書管理

11.1　　文書管理手順の確立及び維持

会社は，CSMS に関連するすべての文書及びデータを管理する手順を確立し，維持しなければならない。

11.2　　文書管理手順の要件

会社は，文書管理手順において，次のことを確保しなければならない。
-1. 有効な文書がすべての関連部署で使用されていること，
-2. 文書の変更は，関係する責任者によって審査されており，承認されていること，及び
-3. 廃棄された文書はすみやかに取り除かれていること。

11.3　　サイバーセキュリティマネジメントマニュアル

CSMS を記述し，実施するために使用される文書を“サイバーセキュリティマネジメントマニュアル”という。また，文書化は，会社が最も効果的と判断する様式としなければならない。各船舶は，自船に関する全文書を船内に備えなければならない。

12 章　会社による検証，見直し及び評価

12.1　サイバーセキュリティマネジメントシステムの監査

会社は，サイバーセキュリティの活動が CSMS に従っているかどうかを検証するため，会社と船舶に対し 12 ケ月を超えない間隔で内部サイバーセキュリティ監査を実施しなければならない。特別の場合は，この間隔は 3 ヶ月を超えない範囲で延期できる。

12.2　供給者関係

会社は，委託された CSMS に関連する業務を引き受けた全ての者たちが，CSMS 下に於ける会社の責任に従って活動しているかどうか定期的に検証しなければならない。

12.3　サイバーセキュリティマネジメントシステムの評価

会社は，設定した手順に従って CSMS の効果を，定期的に評価しなければならない。

12.4　監査及び是正措置の実施

監査及び是正措置は，文書化した手順に従って実施しなければならない。

12.5　監査の独立性

監査を行う者は被監査部署から独立していなければならない。

12.6　レビュー結果の注意喚起

会社は，監査及び見直しの結果について，関係する部署のすべての責任者に対して注意喚起をしなければならない。

12.7　是正措置の実施

関係する部署の責任者は，見出された欠陥に対し時宜を得た是正措置を講じなければならない。

第 2 部　　管理策

1 章　一般

1.1　　目的

第 2 部では, 運航におけるサイバーリスクに適切に対応するために会社及び船舶において実施するサイバーセキュリティ管理策（以降「管理策」という。）を定める。

1.2　　適用

第 2 部は，会社及び船舶に適用する。

1.3　　サイバーセキュリティに係るリスクマネジメントと管理策の関係

1.3.1　　船舶におけるサイバーセキュリティの脅威

船舶の運航に係る船上の装置に，主機関，操舵装置，航行支援装置，発電機，荷役管理に係る装置，情報システム及び端末，通信装置，非常対応に係る装置等がある。これらの装置は，その制御，通信及び人とのインタフェースにおいて ICT を活用しており，特に，ネットワークをとおして装置と外部，また装置同士が接続されている。例えば，主機関は船橋から遠隔制御が行われる。操舵指示は船内ネットワークをとおして操舵装置へ伝達され，また，舵の状態が航行支援装置に表示される。船舶の位置・速度や他の船舶との距離が GPS コンパス，ジャイロコンパス，レーダー等の機器で把握され，航行支援装置に表示される。また，貨物制御及び船内外の通信に ICT が活用されている。

情報通信技術の導入に伴い，船舶の運航において以下を含む様々なサイバーセキュリティの脅威が想定できる。

-1.　船上の装置がネットワークをとおして外部に接続されている場合，装置がサイバー攻撃の対象となり，実際にサイバー攻撃を受けた場合，機器が停止し又は機器の動作に異常が生ずる結果，船舶の正常な運航が損なわれる可能性が生じる。

-2.　無線通信の妨害や通信を介した DoS 攻撃等を受け，航行支援装置が正常に稼働せず，航行に支障をきたす可能性が生じる。

-3.　各種サイバー攻撃により主機関，舵その他の装置の遠隔制御機能が損なわれ，運航における安全が脅かされる可能性が生じる。

-4.　電子メールの利用に伴い，端末や情報システムがウィルス（マルウェア）に感染したり，外部からの攻撃の契機を与えたりする可能性が生じる。

-5.　陸上の情報通信システムがサイバー攻撃を受けることにより，陸上のシステムが保有するデータが漏洩・搾取されたり，陸上のシステムから船内のシステムが攻撃を受けたりすることにより，船舶の正常な運航が損なわれる可能性が生じる。

-6.　人為ミスによる船内システムの誤った構成変更や船員による無意識なサイバー攻撃の組み込みにより, 船舶の正常な運航が損なわれる可能性が生じる。

1.3.2　　サイバーリスクマネジメント

船舶の運航において，サイバーセキュリティとは，運航に係る装置，情報通信機器（情報システム，端末及びネットワーク機器を含む）及び情報を脅威から保護することによって運航の安全を確保するとともに船上業務の適切な遂行を維持するために，会社及び船舶において行う活動をいう。

脅威が具体的な事象として発現し，航行の安全又は船上業務の適切な遂行が損なわれる事態をインシデントという。想定するそれぞれのインシデントに備えて，安全を確保するための対策を講ずる必要がある。

船舶の航行におけるサイバーリスクマネジメントとは，航行の安全及び船上業務の適切な遂行について目標を設定し，

これを達成するための一連の活動をいう。サイバーリスクマネジメントには，以下のプロセスを含む。

- 状況の把握
- リスクアセスメント
- リスク対応

-1. 状況の把握

船舶について以下の状況を把握し，文書化する。

(1) 搭載する装置及びその仕様

装置には，主機関，操舵装置，航行支援装置，発電機，荷役管理に係る装置，非常対応に係る装置を含む。把握し文書化する内容に，以下を含む。

(a) それぞれの装置における ICT の利用

(b) 遠隔制御機能及び自動制御機能の搭載

(2) 搭載する情報通信機器（情報システム，端末及びネットワーク機器を含む）及びその仕様

(3) ネットワーク構成及び通信の使用

ネットワークに接続する装置及び情報通信機器，通信方式・通信内容，及び，インターネット等による船外とのネットワーク接続を含む。

[参照 : IACS Recommendations, No. 156 (Sep 2018) Network Architecture, No. 159 (Sep 2018) Network security of onboard computer based systems]

-2. リスクアセスメント

リスクアセスメントのプロセスについては JIS Q 31000:2010 リスクマネジメント－原則及び指針を参照することが望ましい。

(1) サイバーリスクの特定

船舶の運航に関わる装置，情報通信機器及び情報に影響を与えるサイバーリスクを認識し，記述する。サイバーリスクの特定の際には，業界における最新のサイバーセキュリティに関する情報の把握や，サイバーセキュリティに関する的確な知識を持った人員が参画することが望ましい。また，代表的な情報システムに対するリスク特定の参考例として「附属 2 海事分野における ICT 活用とサイバーリスク」を参考にすることができる。

(2) サイバーリスクの分析

特定されたサイバーリスクに対して，対象の船舶及び会社に対する起こりやすさや影響の度合いを検証する。船舶あるいは積荷の種類，または予定している航路など対象が置かれたビジネス状況により，分析結果は大きく異なることが想定される。また，サイバーリスク間の依存関係も明確にすることで，サイバーリスクの評価のための情報を整備する。

(3) サイバーリスクの評価

分析の結果から，どのリスクへの対応が必要か，またその優先順位を検討する。会社があらかじめ設定したリスク基準との差異を明確にし，個々のリスクへの対応の必要性を検討する。リスク基準とは，リスクの重大性を評価するための目安とする条件(ISO/IEC 31000)であり，規格，法律などからの影響も考慮される。

-3. リスク対応

会社は一連のリスクアセスメントの結果から，サイバーリスク対応の内容を決定する。対応には必要な全ての管理策を選定し，実装することが必要となる。第 2 部は管理策およびその実践の手引きを記載している。一部の管理策は船舶の運航に関わる装置，情報通信機器に関するものを含むため，管理策の実践には造船時点での実装が必要な場合がある。そのため造船時点において実施が必要な管理策と，運行時において実施が必要な管理策を分別し，第 2 章に造船における管理策をまとめている。また，船舶の運航には，会社として組織に対する管理策の他，船舶の運航を支援する陸上に対する管理策も不可欠であるため，第 3 章に運航における会社の管理策，第 4 章に運航における船舶の管理策を記載している。

2 章　造船における管理策

2.1　　サイバーセキュリティのための機能及び運用

目的

造船にあたって，サイバーセキュリティに係るリスク対応（1.3.2 -3.）において選定した管理策を実現することにより，サイバー攻撃を含む脅威から船舶を保護するため。

2.1.1　　サイバーセキュリティのための機能及び運用の設計

-1.　管理策

会社は，船舶に搭載する装置，情報通信機器（情報システム，端末及びネットワーク機器を含む）及びこれらをつなぐネットワーク，並びにこれらを設置する区域について，総合的なサイバーセキュリティのための機能及び運用を設計し，文書化する。

[参照：IACS Recommendations, No. 160 (Nov 2018) Vessel System Design]

-2.　実施の手引

船舶に搭載する装置，情報通信機器及びネットワークの全体を対象として，サイバーリスクに対応するための機能及び運用を設計し，文書化する。この文書を設計方針書（Design Philosophy Document, DPD）という。

会社は，造船においてサイバーセキュリティに係るリスクアセスメント及びリスク対応のプロセスを実施し，必要な管理策を決定する（1.3）。例えば，機器の冗長化やネットワークの分離等，システム構成に係る要件を管理策として決定する。また，それぞれの装置，情報通信機器及びネットワークにおける対策も管理策として具体化する（1.3，2.2，2.3，及び 2.4）。これらのサイバーセキュリティに係るリスクアセスメント及びリスク対応のプロセスは，造船において総合的なサイバーセキュリティのための機能及び運用を設計するプロセスである。

設計方針書には，例えば以下を含める。

(1)　船舶に搭載する装置，情報通信機器及びネットワーク
(2)　装置及び情報通信機器について，そのシステムの分類（「鋼船規則検査要領 D 編 機関」(2018 年),「附属書 D18.1.1 コンピュータシステム」を参照）
(3)　システムの分類を考慮して決定した，安全に関係する要求事項
(4)　条約及び法令に基づく要求事項
(5)　乗組員の知識・技量についての前提
(6)　システム・アーキテクチャに係る前提，例えば単一障害点の回避
(7)　これらの要求事項及び前提に合致し，またリスクアセスメント及びリスク対応をとおして決定したサイバーセキュリティのための機能及び運用

サイバーセキュリティのための機能及び運用は，本章で以下に挙げる管理策及びその他の管理策も検討することによってさらに具体化する。

本管理策は，会社が統合者等に行わせることもある。

2.1.2　　サイバーセキュリティのための機能の実装

-1.　管理策

会社は，船舶に搭載する装置，情報通信機器及びこれらをつなぐネットワーク，並びにこれらを設置する区域について，総合的なサイバーセキュリティのための機能を実装する。

[参照：IACS Recommendations, No. 160 (Nov 2018) Vessel System Design]

-2.　実施の手引

前項「2.1.1 サイバーセキュリティのための機能及び運用の設計」に基づき設計した機能を，装置，情報通信機器及びネットワークに実装する。

2.1.3　　装置等の目録

-1.　管理策

会社は，船舶に搭載する装置，情報通信機器及びこれらをつなぐネットワークの目録を作成し，維持する。

[参照：IACS Recommendations, No. 161 (Sep 2018) Inventory List of computer based systems]

-2. 実施の手引

造船において，船舶に搭載する装置，情報通信機器及びネットワークの決定にあわせて，これらの目録を作成し，維持する。目録には，これらを特定する情報，設置場所，及びネットワーク構成を含める。これらの情報は，関係する管理策及びその実装を決定するための基礎情報となる。

装置及び情報通信機器にソフトウェアを搭載している場合は，ソフトウェアを特定する情報及びバージョンと適用している更新及び修正も記録する。この情報は，ソフトウェアに関する脆弱性が広報され，修正が配布された場合に，修正の適用を管理するために利用する。

2.2 装置

目的

船舶に搭載する装置に対するサイバー攻撃を含む脅威への備えとして，装置に係るサイバーセキュリティ対策を確保するため。

2.2.1 装置の選定

-1. 管理策

会社は，船舶に搭載する装置として，サイバーセキュリティ対策を備えたものを選定する。

-2. 実施の手引

船舶に搭載する装置には，主機関，操舵装置，航行支援装置，発電機，荷役管理に係る装置，非常対応に係る装置等がある。これらの装置が遠隔操作や自動化の機能を持つ場合には，そのための通信やソフトウェアによる制御が行われ，このことが外部からの攻撃に対する脆弱性になりうる。

遠隔操作及び自動化のための通信路は，外部からの侵入を防ぐために，ネットワークセグメントを適切に分離し，その他の用途で利用されるネットワークから隔離する。

ソフトウェア（ファームウェアを含む）を内蔵する装置においては，ソフトウェアの更新及びセキュリティ修正適用の必要性を判断する。必要な更新及びセキュリティ修正が継続的に提供され，適用できる装置を選定する。選定にあたっては，更新及び修正を適用する時及び人員を決定する。例えば，寄港時に当該装置の保守を委託する業者に更新及び修正の適用を行わせることが考えられる。

[参照：IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board]

備えるべきサイバーセキュリティ対策の機能は装置によって異なるが，次の例がある。

(1) 装置の利用方法に応じてセキュリティ設定が選択できる。
(2) ウィルス対策の機能を持つか，ウィルス対策ソフトウェアが導入できる。
(3) 異常及びインシデントの発生について，その検知と状況把握のために有用な監視ができる。
(4) 異常及びインシデントの発生について，その検知と状況把握のために有用なログが取得できる。
(5) 検知した異常やインシデントが船舶の運航に重篤な場合は，装置のネットワークからの切り離しや緊急対応を実施できる。

2.2.2 装置の設定

-1. 管理策

会社は，船舶に搭載する装置に必要なセキュリティ設定を特定し，これを施す。

-2. 実施の手引

必要なセキュリティ設定は装置によって異なるが，次の例がある。

(1) ソフトウェアは，最新の版を採用し，セキュリティ修正を適用する。
(2) 内蔵するシステムの設定は，装置の利用方法に応じてセキュリティが確保できるものを選択する。
(3) 使わない通信ポートを遮断することを含む脆弱性対策を行う。
(4) ウィルス対策を導入する。
(5) 異常の検知及びインシデントの発生検知と状況把握のために有用な監視を有効にする。

(6) 異常の検知及びインシデントの発生検知と状況把握のために有用なログの取得を有効にする。
(7) 検知した異常やインシデントが重篤な場合に対応するため，緊急対応などを実施できる機能を有効にする。

2.2.3 装置の設置

-1. 管理策

会社は，環境上の脅威等からのリスク並びに認可されていないアクセスの機会を低減するように装置を設置する。

-2. 実施の手引

装置を適切に設置するために，次の例がある。

(1) 装置は，作業領域への不要なアクセスが最小限になるように設置する。
(2) 認可されていないアクセスを回避するため，保管設備のセキュリティを保つ。
(3) 特別な保護を必要とする装置は，それ以外の装置と区別して設置・保護する。
(4) 装置設置場所には，潜在的な物理的及び環境的脅威［例えば，水（又は給水の不具合），じんあい（塵埃），振動，電力供給の妨害，通信妨害，電磁波放射，破壊］のリスクを最小限に抑えるための管理策を採用する。
(5) 装置設置場所の運用に悪影響を与えることがある環境条件（例えば，温度，湿度）を監視する。
(6) 作業現場などの環境にある装置には，特別な保護方法（例えば，キーボードカバー）の使用を考慮する。

2.2.4 装置における手動制御機能の装備

-1. 管理策

船舶に搭載する装置であってその制御を遠隔から又は自動的に行うものにおいては，当該制御が不能となった場合に備え，手動による制御の機能を備える。

-2. 実施の手引

主機関，舵その他の装置において，その制御を船橋等離れた区域に置かれた管理システムで管理し，あるいは，制御を装置に内蔵するソフトウェアによって自動化している。このような装置の稼働を確保するため，管理システム又は内蔵ソフトウェア等から独立した，手動による制御のための機能を当該装置に備える。

[参照：IACS Recommendations, No. 154 (Sep 2018) Recommendation concerning manual / local control capabilities for software dependent machinery systems]

2.3 情報通信機器

目的

船舶に搭載する情報通信機器の脆弱性を利用するサイバー攻撃を含む脅威への備えとして，情報通信機器に係るサイバーセキュリティを確保するため。

2.3.1 情報通信機器の選定

-1. 管理策

会社は，船舶に搭載する情報システム及び端末を含む情報通信機器として，サイバーセキュリティ対策の機能を備え，サイバーセキュリティ対策の設定及び実施ができるものを選定する。

-2. 実施の手引

情報通信機器には，情報システム，端末及びネットワーク機器を含む。

船舶に搭載する情報通信機器について，ソフトウェアの更新及びセキュリティ修正が継続的に提供され，適用できるものを選定する。選定にあたって，更新及び修正を適用する時及び者を決定する。例えば，寄港時に当該情報通信機器の保守を委託する業者に更新及び修正の適用を行わせることが考えられる。

[参照：IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board]

備えるべきサイバーセキュリティ対策の機能に，次の例がある。

(1) 情報通信機器の利用方法に応じてセキュリティ設定が選択できる。
(2) ウィルス対策の機能を持つか，ウィルス対策ソフトウェアが導入できる。
(3) 異常及びインシデントの発生について，その検知と状況把握のために有用な監視がきる。
(4) 異常及びインシデントの発生について，その検知と状況把握のために有用なログが取得できる。
(5) 検知した異常やインシデントが船舶の運航に重篤な場合は，ネットワーク接続の遮断や緊急対応を実施できる。

2.3.2 情報通信機器の設定

-1. 管理策

会社は，船舶に搭載する情報通信機器に必要なセキュリティ設定を特定し，これを施す。

-2. 実施の手引

必要なセキュリティ設定に，次の例がある。

(1) ソフトウェアは最新のバージョンを採用し，更新及びセキュリティ修正を適用する。

(2) 使わない通信ポートを遮断することを含む脆弱性対策を行う。

(3) ウィルス対策を導入する。

(4) 異常の検知及びインシデントの発生検知と状況把握のために有用な監視を有効にする。

(5) 異常の検知及びインシデントの発生検知と状況把握のために有用なログの取得を有効にする。

(6) 検知した異常やインシデントが重篤な場合に対応するため，緊急対応などを実施できる機能を有効にする。

2.3.3 情報通信機器の設置

-1. 管理策

会社は, 環境上の脅威等からのリスク並びに認可されていないアクセスの機会を低減するように情報通信機器を設置する。

-2. 実施の手引

情報通信機器を適切に設置するために，次の例がある。

(1) 情報通信機器は，作業領域への不必要なアクセスが最小限になるように設置する。

(2) 認可されていないアクセスを回避するため，保管設備のセキュリティを保つ。

(3) 機器設置場所には，潜在的な物理的及び環境的脅威［例えば，水（又は給水の不具合），じんあい（塵埃），振動，電力供給の妨害，通信妨害，電磁波放射，破壊］のリスクを最小限に抑えるための管理策を採用する。

(4) 機器設置場所の運用に悪影響を与えることがある環境条件（例えば，温度，湿度）を監視する。

(5) 作業現場などの環境にある情報通信機器には，特別な保護方法（例えば，キーボードカバー）の使用を考慮する。

2.4 ネットワーク

目的

船舶に搭載するネットワークにおける脆弱性を利用するサイバー攻撃を含む脅威への備えとして, ネットワークに係るサイバーセキュリティ対策を確保するため。

2.4.1 ネットワークの設計

-1. 管理策

会社は，船舶に搭載するネットワークにおけるサイバーセキュリティ対策を設計する。

-2. 実施の手引

船舶に搭載するネットワークにおけるサイバーセキュリティ対策の設計は, 以下を考慮したリスクマネジメントに基づき実施する。

(1) ネットワークに接続する装置及び情報通信機器とその機能

(2) 装置及び情報通信機器の間で行う通信の必要性と内容

(3) 装置及び情報通信機器と船外との間で行う通信の必要性と内容

(4) 通信に関係する脅威及び脆弱性

ネットワークにおける対策の例に，以下がある。

(5) ネットワーク及び情報通信機器の物理的保護

(6) 通信の暗号化

(7) ネットワーク及びネットワークセグメントの分割

(8) ファイアウォール，スイッチ等による通信のフィルタリング及び通信経路の制御

(9) ウィルス対策

(10) ネットワークへのアクセスにおける認証

(11) 侵入防止システム（Intrusion Prevention System, IPS）による不正侵入の防止，通知及びログ取得

[参照：IACS Recommendations, No. 156 (Sep 2018) Network Architecture, No. 159 (Sep 2018) Network security of onboard computer based systems, No. 162 (Sep 2018) Integration]

特に，運航の安全に関係する以下を含む装置については，陸上との通信，制御のための通信に伴うサイバーリスクを慎重に検討し，対策を決定する必要がある。

(12) ブリッジシステム／航行支援装置

(13) 主機関制御システム

(14) 船橋操縦

(15) 操舵装置／自動操舵装置

(16) 電子海図表示装置

(17) 貨物制御

(18) バラスト制御

[参照：IACS Recommendations, No. 164 (Nov 2018) Communication and Interfaces]

2.4.2 ネットワークの実装

-1. 管理策

会社は，船舶に搭載するネットワークにおけるサイバーセキュリティ対策を実装する。

-2. 実施の手引

船舶に搭載するネットワークにおけるサイバーセキュリティ対策を，その設計（2.4.1）に基づき実装する。

2.5 情報

目的

運航の制御及び管理，並びに船上の業務に係る情報について，サイバー攻撃を含む脅威への備えとして，情報の用途及び重要性に応じた保護を実施するため。

2.5.1 情報の保護

-1. 管理策

会社は，船舶の運航に係る情報（注記）についてその保護の要件を決定し，保護策を設計し，実装する。

[参照：IACS Recommendations, No. 157 (Sep 2018) Data assurance]

注記　IACS Recommendation, No. 157 における「データ（data）」を，本節 2.5 では「情報」としている。

-2. 実施の手引

船舶の運航に係る情報について，その保護の要件を決定し，要件に合致した保護策を設計し，実装する。対象とする情報は，船舶の装置，情報通信機器及びネットワークで取り扱われる。

情報に係る保護の要件は，情報の機密性，完全性及び可用性の要件として，それぞれの要求の程度を例えば「高」「中」「低」と表現することができる。情報に係る保護の要件は，「鋼船規則検査要領 D 編 機関」(2018 年)の「附属書 D18.1.1 コンピュータシステム」に定めるシステムの分類に関係する。IACS Recommendations, No. 157 (Sep 2018) Data assurance において，システムの分類Ⅰ，Ⅱ，Ⅲのそれぞれについて，機密性，完全性及び可用性の要件との関係を次のとおりに例示している。船舶のそれぞれの情報について保護の要件を決定するときに，この例示も参考にすることができる。

システムの分類	機密性の要件	完全性の要件	可用性の要件
Ⅰ	低	中	低
Ⅱ	中	高	中
Ⅲ	中	高	高

情報の保護策は，当該情報を取り扱う装置，情報通信機器及びネットワークにおけるサイバーセキュリティのための機能及びその運用（2.2，2.3 及び 2.4）によって実現する。

情報は，その状態によって，装置又は情報通信機器に保存されている情報と通信途上にある情報がある。それぞれに合致したアクセス制御，暗号化等の対策を決定し，実装する。

2.6 アクセス制御

目的

運航の制御及び管理，並びに船上の業務に関わる情報，船舶に搭載する設備，情報通信機器，及びネットワークへのアクセスを制限するため。

2.6.1 アクセス制御方針

-1. 管理策

会社は，アクセス制御方針を業務におけるセキュリティの要求事項に基づいて確立し，文書化し，レビューする。

-2. 実施の手引

アクセス制御は，論理的又は物理的（2.7）なものであり，この両面を併せて考慮する。会社は，アクセス制御によって達成する業務上の要求事項を明確に規定して提供する。

アクセス制御方針では，次の事項を考慮する。

(1) 業務用アプリケーションのセキュリティ要求事項
(2) 異なる情報システム及びネットワークにおける，アクセス権と情報分類の方針との整合性
(3) ネットワーク環境におけるアクセス権の管理
(4) アクセス制御における役割の分離（例えば，アクセス要求，アクセス認可，アクセス管理）
(5) アクセス要求の正式な認可に対する要求事項
(6) アクセス権の削除
(7) 利用者の識別情報及びアクセス認証情報の利用及び管理に関する，全ての重要な事象の記録の保管
(8) 特権的アクセスを認められた役割

2.6.2 ネットワークへのアクセス

-1. 管理策

会社は，利用することを特別に認可したネットワーク（ネットワークが提供するサービスも含む）へのアクセスだけを利用者に提供する。

-2. 実施の手引

ネットワークの利用に関し，方針を設定する。この方針は，次の事項が例とされる。

(1) アクセスが許されるネットワーク
(2) 誰がどのネットワークへのアクセスが許されるかを決めるための認可手順
(3) ネットワーク接続へのアクセスを保護するための運用管理面からの管理策及び管理手順
(4) ネットワークへのアクセスに利用される手段（例えば，VPN，無線ネットワーク）
(5) 様々なネットワークサービスへのアクセスに対する利用者認証の要求事項
(6) ネットワークサービスの利用の監視

2.6.3 利用者登録及び登録削除

-1. 管理策

アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施する。

-2. 実施の手引

利用者 ID を管理するプロセスには，次の事項が例となる。

(1) 利用者と利用者自身の行動とを対応付けすること，及び利用者がその行動に責任をもつことを可能にする，一意な利用者 ID の利用。共有 ID の利用は，業務上又は運用上の理由で必要な場合にだけ許可し，承認し，記録する。
(2) 組織を離れた利用者の利用者 ID の，即座の無効化又は削除
(3) 必要のない利用者 ID の定期的な特定，及び削除又は無効化
(4) 重複する利用者 ID を別の利用者に重複する利用者 ID を発行しないことの確実化

2.6.4 特権的アクセス権の管理

-1. 管理策

会社は，特権的アクセス権の割当て及び利用は，制限し，管理する。

-2. 実施の手引

特権的アクセス権の割当ては，関連するアクセス制御方針（2.6.1）に従って，正式な認可プロセスによって管理する。

2.6.5 利用者のアクセス認証情報の管理

-1. 管理策

会社は，アクセス認証情報の割当てを，正式な管理プロセスによって管理する。

-2. 実施の手引

アクセス認証情報の割当てには，以下を考慮する。

(1) 利用者に各自のアクセス認証情報を保持することを求める場合，最初に，セキュリティが保たれた仮のアクセス認証情報を発行し，最初の使用時にこれを変更させる。

(2) 新規，更新又は仮のアクセス認証情報を発行する前に，利用者の本人確認の手順を確立する。

(3) 仮のアクセス認証情報は，セキュリティを保った方法で利用者に渡す。外部関係者を通して渡すこと又は保護されていない（暗号化していない）電子メールのメッセージを利用することは避ける。

(4) 仮のアクセス認証情報は，一人一人に対して一意とし，推測されないものとする。

(5) 利用者は，アクセス認証情報の受領を知らせる。

(6) 業者があらかじめ設定したアクセス認証情報は，システム又はソフトウェアのインストール後に変更する。

2.6.6 アクセス権の削除又は修正

1. 管理策

会社は，情報，情報通信機器，及びネットワークに対するアクセス権を，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正する。

-2. 実施の手引

雇用の終了時に，情報，情報通信機器，及びネットワークに関連する資産に対する個人のアクセス権を削除又は一時停止する。雇用を変更した場合，新規の業務において承認されていない全てのアクセス権を削除する。削除又は修正が望ましいアクセス権には，物理的な及び論理的なアクセスに関するものを含む。アクセス権の削除又は修正は，鍵，身分証明書，情報処理機器又は利用登録の，削除，失効又は差替えによって行うことができる。従業員及び契約相手のアクセス権を特定するあらゆる文書に，アクセス権の削除又は修正を反映する。退職する従業員又は外部の利用者が引き続き有効な利用者 ID のアクセス認証情報を知っている場合，雇用・契約・合意の終了又は変更に当たって，これらの情報を変更することが望ましい。

2.6.7 セキュリティに配慮したログオン手順

-1. 管理策

会社は，アクセス制御方針で求められている場合には，情報，設備，情報通信機器，ネットワークへのアクセスは，セキュリティに配慮したログオン手順によって制御する。

-2. 実施の手引

利用者が提示する識別情報を検証するために，適切な認証技術を選択する。強い認証及び識別情報の検証が必要な場合には，パスワードだけではなく，暗号による手段，スマートカード，トークンデバイス，生体認証などの認証方法を組み合わせて用いることも考慮する。

ログオンするための手順は，認可されていないアクセスの機会を最小限に抑えるように設計する。したがって，ログオン手順では，認可されていない利用者に無用な助けを与えないために，システム又はアプリケーションについての情報の開示は，最小限にする。

2.6.8 リモートアクセス及びリモートアップデート

-1. 管理策

会社は，船舶に搭載する装置及び情報通信機器に対するリモートアクセス及びにリモートアップデート係るサイバーセキュリティの方針を作成し，対策を実施する。

-2. 実施の手引

装置及び情報通信機器は，以下の目的で遠隔からアクセスする場合がある。

(1) 装置及び情報通信機器の状態を監視する。

(2) 装置及び情報通信機器の状態を診断する。

(3) 装置及び情報通信機器のソフトウェア及びデータを更新する。

これらのアクセス及び処理は，以下のような脅威を伴う。

(4) アクセスのための通信路が悪用され，侵入その他の攻撃を受ける。

(5) 監視及び診断のために付与される管理者権限又はその他のアクセス権が悪用されたり，このアクセス権の下で誤操

作が行われたりして，装置又は情報通信機器の正常な稼働が損なわれる。
(6) ソフトウェア及びデータの更新処理が失敗し，装置又は情報通信機器の正常な処理が損なわれる。
(7) 更新後のソフトウェア又はデータに誤りその他の問題が含まれているために更新後に正常な処理が損なわれる。
(8) ソフトウェア又はデータの更新に伴って装置又は情報通信機器がウィルスに感染する。
これらの脅威に対処するため，リモートアップデート及びリモートアクセスに係るサイバーセキュリティの対策を定め，これを実施する。対策には，以下の例がある。
(9) 対象とする装置及び情報通信機器と，実施する処理の特定
(10) アクセス及び通信における認証，アクセス制御及び通信の暗号化
(11) 実施する事業者及び人員の特定と責任者の指定
(12) 実施に係る運用面の管理，例えば，事前申請及び教育
(13) 実施記録の取得とその確認
[参照：IACS Recommendations, No. 163 (Sep 2018) Remote Update / Access]

2.7 物理的対策

目的
船舶に搭載する装置，情報通信機器及びネットワークに係る誤操作，破壊，毀損その他の脅威への備えとして，区域の管理を含む物理的サイバーセキュリティ対策を確保するため。

2.7.1 区域

-1. 管理策
会社は，サイバーセキュリティ対策のための船内の区域を設定し，区域について物理的対策を実施する。
[参照：IACS Recommendations, No. 158 (Oct 2018) Physical Security of onboard computer based system]
-2. 実施の手引
区域の物理的対策についての方針を策定する。方針において，例えば以下の事項を定める。
(1) 保有する装置，情報通信機器及びネットワークに応じた区域の設定
(2) 区域への立ち入りを許可する者及び時
区域の物理的対策を決定し，実装する。区域の物理的対策には，次の例がある。
(3) 区域の境界に壁を設け，区域への立ち入りを制限する。
(4) 区域の扉に鍵を設け，立ち入る者を制限する。
(5) 鍵の使用に係るログを取得し，立入りの記録をとる。
(6) 記録へのアクセスを管理し，記録を保護する。

2.7.2 装置，情報通信機器及びネットワークの物理的保護

-1. 管理策
会社は，装置，情報通信機器及びネットワークを保護する物理的対策を決定し，実施する。
[参照：IACS Recommendations, No. 158 (Oct 2018) Physical Security of onboard computer based system]
-2. 実施の手引
装置，情報通信機器及びネットワークを保護する物理的対策に以下の例がある。
(1) 装置，情報通信機器及びネットワークを適切な物理的対策を備えた区域に設置する。
(2) 電源，通信設備，空調設備の稼働を確保するため，必要に応じこれらを冗長化する。
(3) 機器等を許可なく区域から持ち出させない。

2.8 緊急事態対応計画（コンティンジェンシー・プラン）

目的
サイバーセキュリティに係る緊急事態をあらかじめ想定して対応を計画することによって，緊急事態がもたらす損害を低減するため。

2.8.1 緊急事態対応計画の策定

-1. 管理策

会社は，サイバーセキュリティに係る緊急事態対応計画を整備する。

[参照：IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems]

-2. 実施の手引

緊急事態対応計画には，次の内容を含む。

(1) 当該計画の対象とする装置及び情報通信機器の一覧

(2) インシデント対応計画

(3) 復旧計画

緊急事態対応計画の整備にあたり，対象とする装置及び情報通信機器を決定し，一覧にする。決定にあたり，運航の安全における当該装置又は情報通信機器の重要性や想定されるインシデントの影響を判断の材料とする。また，業界指針等における規定に留意する。

インシデント対応計画には，次の内容を含める。

(1) 想定するインシデントの種類とインシデントの記述

(2) 陸上及び船舶における連絡体制と連絡内容

(3) 専門業者を含む外部組織との連携

(4) インシデント発生時の措置

復旧計画には，次の内容を含める。

(1) 装置及び情報通信機器の復旧手順

(2) 情報の復旧手順

(3) 専門業者を含む外部組織との連携

策定した緊急事態対応計画は会社及び船舶において試行し，検証する。また，必要な改善を反映する。

緊急事態対応計画は，会社及び船舶に備える。

2.9 供給者関係

目的

造船において委託する業務及び調達する装置･機器等について,運航に対するサイバー攻撃を含む脅威への備えとして，サイバーセキュリティ対策の実施及び実装を確保するため。

2.9.1 供給者関係におけるサイバーセキュリティの要求事項の提示

-1. 管理策

調達者は，造船における業務の委託及び調達にあたって，サイバーセキュリティのための要求事項への適合を供給者に求める。

-2. 実施の手引

船舶所有者又は船舶管理者等である会社は，造船を統合者に委託する。統合者は，船舶に搭載する装置，情報通信機器及びネットワークを供給者から機器として調達したり，これらを構築する業務を供給者に委託したりする。

本管理策は，会社及び統合者等が造船における業務の一部を委託する場合に，委託元・調達元である会社，統合者等に適用する。船舶の所有者となる会社は，統合者との契約を通して，本管理策を統合者に実施させる。

造船における業務の委託にあたって，サイバーセキュリティのための要求事項として，以下を委託契約に含めることが考えられる。

(1) 装置，情報通信機器及びネットワークに具備するサイバーセキュリティのための機能

(2) 委託先における作業体制及び作業環境に関する要求事項

委託先に求めるサイバーセキュリティのための要求事項を決定するために，装置，情報通信機器及びネットワークに係る管理策とその実施の手引（2.2，2.3，2.4）を参考にすることができる。

統合者は，装置，情報通信機器又はネットワークを外部から調達する場合がある。このとき，統合者は，求められるサイバーセキュリティの要求事項に適合するものを調達する。

委託先における作業体制及び作業環境に係る要求事項は，委託先における作業の適正を確保するためのものである。納

品物に求める機能の実装及び品質を確保するため，委託先における適切な体制及び管理を求める。また，委託先における作業環境を他の業務から分離することを求めることもある。

調達者は，造船の委託にあたって，サイバーセキュリティについて納品を求める仕様書及び検査成績等を決定し，委託契約に含める。

2.9.2 供給者関係におけるサイバーセキュリティの確保

-1. 管理策

調達者は，造船における業務及び機器等の調達にあたって，納品物がサイバーセキュリティのための要求事項を満たすことを検証する。

-2. 実施の手引

調達者は，検収にあたって，納品物がサイバーセキュリティの要求事項を満たしていることを検証する。

3 章　運航における会社の管理策

3.1　運航規則の整備

目的

船舶の運航において，サイバー攻撃を含む脅威に対して，乗組員がサイバーセキュリティ対策を確実に実施できるようにするため。

3.1.1　運航規則の策定

-1.　管理策

会社は，運航におけるサイバーセキュリティについて，乗組員に適用する規則を策定する。

-2.　実施の手引

乗組員に適用する運用規則は，サイバーセキュリティのための運用（2.1.1）及び装置（2.2），情報通信機器（2.3），ネットワーク（2.4）及び物理的対策（2.5）の各管理策の実施方法に沿って策定する。

3.2　運航における支援及び管理

目的

船舶の運航において，サイバー攻撃を含む脅威に対して，乗組員がサイバーセキュリティ対策を確実に実施できるようにするため。

3.2.1　運航の支援

-1.　管理策

会社は，運航におけるサイバーセキュリティについて，乗組員を支援する。

-2.　実施の手引

乗組員の支援には，以下を含む。

(1)　船舶に搭載する装置，情報通信機器及びネットワークにおけるサイバーセキュリティ対策，並びにサイバーセキュリティに係る物理的対策について，乗組員が必要とする説明文書の作成及び供与

(2)　運航におけるサイバーセキュリティに係る運用規則の策定，並びに当該運用規則の乗組員への供与及び説明（関連する管理策に「4.1.1 運用規則の履行」がある。）

(3)　運航におけるサイバーセキュリティに係る緊急事態対応計画の策定，並びに当該計画の乗組員への供与及び説明（関連する管理策に「4.2.1 緊急事態対応の実施」がある。）

(4)　運用規則及び緊急事態対応計画に加えて乗組員に供与する必要のあるサイバーセキュリティに係る情報の整備及び供与

(5)　運航におけるサイバーセキュリティに係る連絡

3.2.2 運航の管理

-1.　管理策

会社は，運航におけるサイバーセキュリティについて，状況を把握し，管理する。

-2.　実施の手引

運航におけるサイバーセキュリティに係る状況の把握及び管理には，以下を含む。

(1)　運航におけるサイバーセキュリティのための対策について，その実施状況の把握及び管理

(2)　特に，船上の装置及び情報通信機器におけるソフトウェアの更新及びセキュリティ修正の適用について，その実施状況の把握及び管理

(3)　サイバー攻撃及びサイバーインシデントの一般的な傾向を含む，船舶の運航に影響を与える可能性のあるサイバーセキュリティの状況の把握

3.3 陸上の情報通信機器におけるセキュリティ対策

目的

船舶の運航におけるサイバー攻撃を含む脅威への備えとして, 運航に関係する陸上の情報通信機器におけるサイバーセキュリティ対策を確実に実施するため。

3.3.1 陸上の情報通信機器の特定

-1. 管理策

会社は, 船舶の運航におけるサイバーセキュリティに関係する情報システム及び端末を含む陸上の情報通信機器を特定する。

-2. 実施の手引

会社は，さまざまな業務のために情報システム及び端末を含む情報通信機器を保有している。これらの情報通信機器の中で, 船舶の運航におけるサイバーセキュリティに関係する情報通信機器を特定する。これに該当する情報通信機器には, 以下を含む。

(1) 船上の装置，情報通信機器及びネットワークの仕様を含む，船舶におけるサイバーセキュリティのための機能及び運用についての文書を管理する機器
(2) 運航における船舶のサイバーセキュリティ対策の状況を管理する機器
(3) 運航における船舶と会社の間の通信に係る機器

3.3.2 陸上の情報通信機器の設定

-1. 管理策

会社は, 船舶の運航におけるサイバーセキュリティに関係する陸上の情報通信機器に必要なセキュリティ設定を特定しこれを施すことを含む，セキュリティ対策を実施する。

-2. 実施の手引

前で特定した陸上の情報通信機器について，セキュリティ対策を設計し，実施する。

特に，情報通信機器に必要なセキュリティ設定に，次の例がある。

(1) ソフトウェアは最新のバージョンを採用し，更新及びセキュリティ修正を適用する。
(2) 使わない通信ポートを遮断することを含む脆弱性対策を行う。
(3) ウィルス対策を導入する。
(4) 異常の検知及びサイバーインシデントの発生検知と状況把握のために有用な監視を行う。
(5) 異常の検知及びサイバーインシデントの発生検知と状況把握のために有用なログを取得する。
(6) 検知した異常やインシデントが重篤な場合に対応するために緊急対応などを実施できるようにする。

3.4 ログ取得及び監視

目的

船舶の運航においてサイバーセキュリティに係るイベントを早期に発見して適切に対応するとともに, 事後調査のための情報を確保するため。

3.4.1 運航におけるサイバーセキュリティの監視

-1. 管理策

会社は，運航中の船舶について，サイバーセキュリティに関するイベントの監視を行う。

-2. 実施の手引

会社は，運航中の船舶における装置（2.2），情報通信機器（2.3），ネットワーク（2.4）及び物理的対策（2.5）について定められたイベントを記録する。イベントを記録したログは，改ざん及び認可されていないアクセスから保護することが望ましい。

3.5 緊急事態対応

目的

運航中の船舶におけるサイバーセキュリティに係る緊急事態において，会社が緊急事態対応計画に従って対応することによって，緊急事態がもたらす損害を低減するため。

3.5.1 緊急事態対応の実施

-1. 管理策

運航中の船舶においてインシデントが発生した場合，会社は，定められた緊急事態対応計画に従って行動する。

[参照：IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems]

-2. 実施の手引

イベント監視を通じて船舶の運航に影響をもたらすインシデントを検知した場合，会社は，定められた緊急事態対応計画に従って行動する。

インシデント対応及び復旧を確実に実施するために，会社は，これらの計画に従った訓練を適時に実施する。

4 章　運航における船舶の管理策

4.1 装置・情報通信機器及びネットワークの管理

目的

運航中の船舶においてサイバーセキュリティのための運用を確実に実施することによって,サイバー攻撃を含む脅威に備えるため。

4.1.1　　運用規則の履行

-1.　管理策

乗組員は，運航におけるサイバーセキュリティについて，定められた運用規則を実施する。

-2.　実施の手引

乗組員は，装置，情報通信機器及びネットワークにおけるサイバーセキュリティに係る業務を，定められた運用規則（3.1.1）に従って実施する。

4.1.2　　ソフトウェアの更新及びセキュリティ修正の適用

-1.　管理策

会社又は乗組員は，定められた手順に従って，船上の装置及び情報通信機器のソフトウェアを更新し，セキュリティ修正を適用する。

-2.　実施の手引

ソフトウェア（ファームウェアを含む）の更新及びセキュリティ修正の適用は，必要な通信速度が確保できる入港時に行うことが考えられる。更新及び修正の適用は，定められた手順に従って，例えば保守を委託する業者に行わせることが考えられる。適用の必要性が特に高い更新及び修正が発行された場合であっても，運航中の船上での適用については極めて慎重に判断し，原則としてこれを行わないことが望ましい。適用にあたって専門家の支援が得られないこと，適用のために装置又は情報通信機器の稼働を停止すること,及び更新又は修正を取得するための通信において通信速度が限られていることを考慮する。

[参照：IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board]

ソフトウェアの更新及びセキュリティ修正を行う者は，予め定めておく。会社からの委託により外部の業者に行わせる場合もある。

4.2　　緊急事態対応

目的

運航中の船舶におけるサイバーセキュリティに係る緊急事態において,船舶の乗組員が緊急事態対応計画に従って対応することによって，緊急事態がもたらす損害を低減するため。

4.2.1　　緊急事態対応の実施

-1.　管理策

運航中の船舶においてインシデントが発生した場合，乗組員は，定められた緊急事態対応計画に従って行動する。

[参照：IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems]

-2.　実施の手引

インシデントが発生した場合，乗組員は，定められた緊急事態対応計画に従って行動する。

インシデント対応及び復旧を確実に実施するために，乗組員は，これらの計画に従った訓練を適時に実施する。

附属書

1　　参考文献

(1) IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board

(2) IACS Recommendations, No. 154 (Sep 2018) Recommendation concerning manual / local control capabilities for software dependent machinery systems

(3) IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems

(4) IACS Recommendations, No. 156 (Sep 2018) Network Architecture, No. 159 (Sep 2018) Network security of onboard computer based systems

(5) IACS Recommendations, No. 157 (Sep 2018) Data assurance

(6) IACS Recommendations, No. 158 (Oct 2018) Physical Security of onboard computer based system

(7) IACS Recommendations, No. 159 (Sep 2018) Network security of onboard computer based systems

(8) IACS Recommendations, No. 160 (Nov 2018) Vessel System Design

(9) IACS Recommendations, No. 161 (Sep 2018) Inventory List of computer based systems

(10) IACS Recommendations, No. 162 (Sep 2018) Integration

(11) IACS Recommendations, No. 163 (Sep 2018) Remote Update / Access

(12) IACS Recommendations, No. 164 (Nov 2018) Communication and Interfaces

(13) JIS Q 27001:2014 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

(14) JIS Q 31000:2010 リスクマネジメント－原則及び指針

2　海事分野における ICT 活用とサイバーリスク

	I. ICT の活用場面	II. 機器	III. 通信	IV. 事象 1：行為，機器の状態，自然現象等	V. 事象 2：結果に至る直接の原因	VI. リスク
1. 航海システム						
1-1	ブリッジシステム，航行支援装置 ・地図及び位置表示／航路表示／他船等の表示 ・航行指示 ・航行制御	GPS コンパス	GPS の位置情報を取得	GPS の位置情報がかく乱される	船速距離計の高周波送受信や GPS 衛星からの信号を妨害する電波 （GPS 信号を利用した武力的攻撃からの防御）	正しい位置情報が使えなくなる 正しい方位情報が使えなくなる 自動操舵が不能になる
1-2		ジャイロコンパス	船速距離計からの船速情報と GPS の位置情報で補正	船速距離計の高周波送受信や GPS の位置情報がかく乱される		
1-3		自動操舵装置	GPS の位置情報を取得 ジャイロコンパスからの方位情報を取得	船速距離計の高周波送受信や GPS の位置情報がかく乱される		
1-4		航海情報記録装置 (Voyage Data Recorder)	GPS 位置，速力，自動操舵装置等の航海データの記録	①船速距離計の高周波送受信や GPS の位置情報がかく乱される ②蓄積したデータを搾取される	船速距離計の高周波送受信や GPS 衛星からの信号を妨害する電波 オプション機能であるが，リアルタイムモニタからの不正侵入	正しい航海データが蓄積できない
1-5		音響測深機 (Echo Sounder)	船底から音波を送受信し，水深を計測	音波をかく乱される	音波妨害	正しい水深が測定できず，乗揚げの危険が増す
1-6		船速距離計 (Doppler Speed Log)	高周波の送受信により，船速を計測	高周波の送受信がかく乱される	高周波の送受信の妨害	正しい速力が計測できず，操船に影響する
1-7		レーダー	レーダー波の送受信により，物標の方位と距離を計測	レーダー波をかく乱される	レーダー波の妨害	周囲の状況を判断できなくなる
1-8		電子海図情報表示装置 (ECDIS)	①電子海図上に GPS の位置情報を表示する ②電子海図のインストールや更新にインターネットや USB を利用	GPS の位置情報がかく乱される マルウェア感染	GPS 衛星からの信号を妨害する電波 インターネットの接続及び USB の使用によるウィルス感染	自船の位置が不明となり，操船に影響が出る
1-9		GPS（Global Positioning System）	衛星から位置情報を受信	GPS の位置情報がかく乱される	GPS 衛星からの信号を妨害する電波	自船の位置が不明となり，操船に影響が出る
1-10		AIS (Automated Identification System)	船名，船位，針路等の情報を，国際 VHF を利用し，周辺船舶や陸上局に自動送信	国際 VHF がかく乱される	VHF 波の妨害	他船情報が不明となり，操船に影響が出る
1-11		BNWAS (Bridge Navigational Watch Alarm System)	オプションで ECDIS 等の航海設備と接続	ECDIS からのウィルス感染	ECDIS からのウィルス感染	当直航海士の居眠りを見過ごし，危険な状況を発生させる危険がある

	I. ICTの活用場面	II. 機器	III. 通信	IV. 事象1：行為，機器の状態，自然現象等	V. 事象2：結果に至る直接の原因	VI. リスク
2. 機関システム						
2-1	機関運転の自動化	主機関コントロールシステム（Main Engine Control System） ボイラ （Boilers）	燃料管理システムとの連携によるインターネットを介した自動監視及び情報送信	攻撃者がシステムに侵入し，攻撃のための情報を窃取する	エンジン制御システムに不正な情報が入力として与えられる。	機関の正常な運転が損なわれる
2-2			主機関コントロールシステムとの接続			
2-3		船橋操縦（Bridge Maneuvering）	船橋からの遠隔操縦に伴うネットワーク接続			
3. 操舵						
3-1	電子化された操舵指示	操舵装置（Steering Gear）	自動操舵装置との接続	不正な操舵信号が入力される	自動操舵装置との接続	正確な操舵が取れなくなる
4. 荷役管理						
4-1	貨物の積み付け	ローディングコンピューター（Loading Computer）	インターネットを介した，陸上との通信	攻撃者がシステムに侵入し，攻撃のための情報を窃取する マルウェア感染	システムに不正な情報が入力として与えられる マルウェア感染	貨物情報の漏洩 船体コンディションを崩し，復原性を失い，転覆の可能性が増す
4-2	船体コンディションの維持	バラスト水処理装置（Ballast Water Management System）	インターネットを介した，陸上との通信			水生生物の移動・拡散を助長
4-3		貨物制御	液化ガスばら積み船の温度・圧力制御 冷凍倉の温度管理・雰囲気制御	ボイルオフガスの増加 生鮮食品貨物の腐敗	液化ガス貨物の温度・圧力上昇 冷凍倉の温度・酸素濃度上昇	貨物量の低下 貨物価値の低下
4-4		バラスト制御	バラストタンクの水位，喫水，傾斜等の情報取得	誤った情報の入力	ウィルス感染	船体コンディションを崩し，復原性を失い，転覆の可能性が増す
5. 情報通信						
5-1	電子メール等による情報伝達・受領	VSAT（Very Small Aperture Terminal）/INMARSAT	衛星通信（インマルサット他）を使用した電子メール，ウェブアクセス等	マルウェア，APT攻撃等（陸上でのインターネット利用において想定される攻撃，異常状態と同じ）	PC，サーバがマルウェアに感染する PC，サーバが攻撃者に侵入されたり操作されたりする	情報が漏洩する 会社，他船舶との連絡が不通または遅延する PCやサーバを使う業務が止まる
6. 非常対応						
6-1	遭難時の対応	GMDSS(Global Maritime Distress and Safety System)	INMARSAT を介したインターネット通信	攻撃者が不正な遭難信号を発信	システムに不正な情報が入力として与えられる	不正な遭難信号が発信される 他船の遭難信号を受信できなくなる
6-2	火災時の対応	火災探知システム（Fire	通信システムとの接続はない	火災	マルウェアに感染する	火災探知の誤作動が発生

	I. ICT の活用場面	II. 機器	III. 通信	IV. 事象 1：行為，機器の状態，自然現象等	V. 事象 2：結果に至る直接の原因	VI. リスク
		Detection system)				する
7. ソフトウェアシステム						
7-1	E メールソフト	船内 LAN	インターネットを介した通信	サイバー攻撃の可能性あり	インターネットを介した通信	情報の漏洩
7-2	海図改補ソフト	ECDIS				操船への影響
7-3	ウェザーインフォメーションソフト	船内 LAN				運航計画への影響
7-4	ローディングコンピューターソフト	ローディングコンピューター	船内 LAN との接続あり	マルウェア感染の可能性あり	船内 LAN との接続	堪航性保持への影響
7-5	積付計画ソフト	船内 LAN に接続された事務室 PC				堪航性保持への影響
7-6	保守整備プログラム	船内 LAN に接続された機関制御室及び事務室 PC				機関正常運転への影響
7-7	燃料管理プログラム	船内 LAN に接続された機関制御室及び事務室 PC	インターネットを介した通信	サイバー攻撃の可能性あり	インターネットを介した通信	経済運航への影響

謝辞

本ガイドラインの策定に当たり，ご指導，ご協力をいただいた以下の委員各位および作業部会のメンバーに深く謝意を表する次第である。

策定委員会名簿

（敬称略，順不同）

委員長：
髙木　健　東京大学大学院 新領域創成科学研究科 海洋技術環境学専攻
海洋技術政策学分野　教授

委員：
河野　省二　日本マイクロソフト（株）　技術統括室　チーフセキュリティオフィサー
中尾　康二　（国研）情報通信研究機構　サイバーセキュリティ研究所　主管研究員
山下　真　（国研）情報通信研究機構　サイバーセキュリティ研究所
サイバーセキュリティ研究室　研究技術員
髙野　裕文　（一財）日本海事協会　常務執行役員 事業開発本部長
有馬　俊朗　（一財）日本海事協会　執行役員 開発本部長
池田　靖弘　（株）シップデータセンター　代表取締役社長

作業部会名簿

（敬称略，順不同）

中尾　康二　（国研）情報通信研究機構　サイバーセキュリティ研究所　主管研究員
山下　真　（国研）情報通信研究機構　サイバーセキュリティ研究所
サイバーセキュリティ研究室　研究技術員
後藤　里奈　日本マイクロソフト（株）パートナー事業本部
パートナービジネス統括本部　ソリューション＆ISV ビジネス本部
ビジネスディベロップメントマネージャー
池田　靖弘　（株）シップデータセンター　代表取締役社長

一般財団法人 日本海事協会 事業開発本部 認証2部

〒102-8567 東京都千代田区紀尾井町4番7号
Tel: 03-5226-2412
Fax: 03-5226-2179
E-mail: qpd@classnk.or.jp

www.classnk.or.jp

February 2019