

CHARTING THE FUTURE 

ClassNK

船舶におけるサイバーセキュリティマネジメント
システム認証ガイドライン

[第 2 版]

[日本語 / Japanese]



ClassNK

Copyright © 2026 Nippon Kaiji Kyokai
禁無断転載

改訂履歴

No.	改訂日付	区分	改訂内容
1.0	2019.3.1	新規	新規作成
2.0	2026.10.2	改訂	全面改訂

目次

序文	1
1 一般	1
2 背景	1
3 本ガイドラインの構成	1
4 定義	1
第1部 要求事項	3
1章 適用範囲及び基本要素	3
1.1 サイバーセキュリティマネジメントの目的	3
1.2 サイバーセキュリティマネジメントシステム(CSMS)の目的	3
1.3 関連する規則、条約、コード及び指針との両立性	3
1.4 適用	3
1.5 サイバーセキュリティマネジメントシステム (CSMS) の構成要素	3
2章 リーダーシップ及び方針に関する要求	4
2.1 サイバーセキュリティ方針の確立	4
2.2 サイバーセキュリティ方針の実施及び維持	4
3章 統治体制及び責任に関する要求	5
3.1 役割及び責任	5
3.2 トップマネジメントの責任	5
3.3 会社サイバーセキュリティ責任者	5
3.4 船舶サイバーセキュリティ責任者	5
3.5 船長の権限	6
4章 経営資源及び能力に関する要求	7
4.1 資源の確保	7
4.2 能力	7
4.3 教育及び訓練	7
5章 サプライチェーンに関する要求	8
5.1 供給者への要求事項	8
5.2 供給者の評価	8
6章 サイバーリスク評価に関する要求	9
6.1 サイバーリスクアセスメントの役割	9
6.2 リスクアセスメントの対象	9
6.3 サイバーリスクアセスメントにおける実施プロセスの管理	9
6.4 サイバーリスクの特定及び評価	9
6.5 サイバーリスクアセスメントの見直し	10
7章 構成管理に関する要求	11
7.1 構成管理	11
7.2 変更管理	11
7.3 構成の見直し	11
8章 管理策	12
8.a アクセス及び利用の管理	12
8.a.1 識別及び認証管理	12

8.a.2	認可及び特権管理	12
8.a.3	リモートアクセス及び第三者アクセスの管理	12
8.a.4	適切な利用及び利用者起因リスクの管理	12
8.b	ネットワーク及び通信の保護	12
8.b.1	ネットワーク分離及びゾーニング	12
8.b.2	通信の保護	12
8.b.3	外部接続の管理	12
8.c	システム構成及び保守	12
8.c.1	安全な構成及びハードニング	12
8.c.2	パッチ及び更新管理	12
8.c.3	陳腐化管理	12
8.c.4	マルウェア及びエンドポイント保護	12
8.c.5	ハードウェア及びソフトウェアの管理	12
8.d	媒体及び物理インターフェース管理	12
8.d.1	可搬媒体の管理	12
8.d.2	物理ポート及びインターフェースの保護	12
8.d.3	直接接続の管理	12
8.d.4	物理アクセスの管理	12
8.e	監視、ログ及び検知	12
8.e.1	イベントログ管理	12
8.e.2	セキュリティ監視	12
8.e.3	ログの保全及び保存	12
8.e.4	ログのレビュー及び異常調査	12
8.f	バックアップ及び復旧	12
8.f.1	バックアップ方針及び実施	12
8.f.2	復旧手順	12
8.f.3	バックアップ及び復旧手順の検証	12
9章	緊急事態対応に関する要求	13
9.1	緊急事態への対応手順の確立	13
9.2	緊急事態への対応プログラムの確立	13
9.3	緊急事態への対応を確保する手段の提供	13
10章	不適合及び是正措置に関する要求	14
10.1	不適合の報告及び分析	14
10.2	是正措置及び再発防止策	14
11章	文書管理に関する要求	15
11.1	文書管理手順の確立及び維持	15
11.2	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、見直し及び評価に関する要求	16
12.1	内部サイバーセキュリティ監査	16
12.2	サイバーセキュリティマネジメントシステムの評価	16
第2部	評価基準及び客観的証拠	17

序文

1 一般

船舶の運航は、デジタルシステム及びネットワークに依存する度合いを高めている。これに伴い、サイバーリスクは、船舶の安全な運航、環境の保護及び運航の継続に直接影響し得る。

こうしたリスクへの対応は、技術的な対策を講じることのみをもって完結するものではない。個々の技術的対策は、それを選択し、維持し、見直すマネジメントの過程があってはじめてその機能を保つ。会社が、方針を定め、体制を整え、リスクを評価し、対策を選択して実施し、その結果を見直すとともに、有事に備える。こうした一連の過程を継続的に運用することによって、はじめて実効性を持つ。

本ガイドラインは、サイバーセキュリティマネジメントシステム（以下、CSMS という。）の要求事項を定めるものである。CSMS は、会社が自社の船舶の運航におけるサイバーリスクに対処するためのガバナンス及びマネジメントの構造を提供する。あわせて、このマネジメントの下で船舶及び船上システムに適用する管理策を **8 章**に定める。管理策の選択及び適用範囲は、**6 章**に定めるサイバーリスクアセスメントの結果に基づき決定される。

2 背景

2017 年、国際海事機関（IMO）は決議 MSC.428(98)を採択し、サイバーリスクを ISM コードに基づく安全マネジメントシステムのもとで管理することを勧告した。本会は、これを受け、2019 年 4 月、ISM コードの枠組みを踏まえた CSMS の要求事項を本ガイドラインの第 1 版として公表した。

第 1 版の発行以降、本会は審査の実施を通じて知見を蓄積してきた。2026 年の第 2 版においては、これを基礎として、組織がサイバーセキュリティを管理するための規格として国際的に広く用いられている ISO/IEC 27001 及び ISO/IEC 27002 を参考に最新化するとともに、本会の審査における評価基準を明確化した。

3 本ガイドラインの構成

本ガイドラインは、**第 1 部**及び**第 2 部**により構成される。**第 1 部**は、CSMS の要求事項を定め、各章の冒頭に、その章が規定する内容の概要を示す。第 1 部第 8 章には、船舶の IT/OT システムを対象とする管理策を分類して示す。**第 2 部**は、**第 1 部**に定める要求事項及び管理策について、本会の審査における評価基準及び求められる客観的証拠を定める。

4 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。

4.1 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。

4.2 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。

4.3 主管庁

船舶の旗国の政府をいう。

4.4 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。

4.5 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。

4.6 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。

4.7 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。

4.8 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。

4.9 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 適用範囲及び基本要求

本章は、本ガイドラインの目的、適用及び CSMS として構築すべき要素を明示するものである。CSMS の構築と運用はここに定める前提の上に成り立つものであり、以降のすべての章はこの土台の上に読まれることを想定している。

1.1 サイバーセキュリティマネジメントの目的

サイバーセキュリティマネジメントの目的は、会社が、船舶運航におけるサイバーリスクを体系的に評価・管理し、運航の安全性、環境保護及び運航継続性を確保することにある。

1.2 サイバーセキュリティマネジメントシステム(CSMS)の目的

サイバーセキュリティマネジメントシステム(CSMS)の目的は、会社が船舶のサイバーセキュリティマネジメントを運用するための仕組みを構築し、実施し、維持し、次の事項を達成することにある。

- 1. 船舶の IT 及び OT システムに関連するサイバーリスクを識別し、評価すること。
- 2. 評価されたサイバーリスクに対し、適切な管理策を決定し実施すること。
- 3. サイバーインシデントへの対応及び復旧並びに緊急事態への準備を確保すること。
- 4. 会社及び船舶におけるマネジメントの有効性を継続的に改善すること。

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
- 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。

1.4 適用

本ガイドラインは、会社及び当該会社が適用対象とする船舶に適用する。

1.5 サイバーセキュリティマネジメントシステム（CSMS）の構成要素

会社は、次の事項を含む 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. リスクアセスメントの実施手順、
- 3. 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、
- 4. 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、
- 5. 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、

- 6. 緊急事態に対する準備及び対応の手順書、及び
- 7. 内部監査及び経営者による見直しに関する手順書。

2 章 リーダーシップ及び方針に関する要求

本章は、サイバーセキュリティ方針の策定及び実行に関する要求を規定するものである。方針は文書として存在すれば足りるものではなく、トップマネジメントのリーダーシップの下で会社の意思として確立され、組織全体で実行されて初めて意味を持つ。

2.1 サイバーセキュリティ方針の確立

会社は、1.2 の目的を達成する方策を含む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 統治体制及び責任に関する要求

本章は、CSMS の運用に必要な役割及び責任を規定するものである。サイバーリスク管理は特定の担当者に委ねて成立するものではなく、トップマネジメントが最終責任を負ったうえで、陸上及び船舶に置かれた責任者を含む運用の体制を定め、その体制の下で各々が役割と責任を果たすことにより、はじめて実効性を持つ。

3.1 役割及び責任

- 1. 会社は、CSMS の有効な実施に必要な役割及び責任を特定し、定義し、文書化しなければならない。これには、本章に規定する会社サイバーセキュリティ責任者及び船舶サイバーセキュリティ責任者を含むが、これらに限定されない。本ガイドラインに定める責任は最低限の要求事項であり、会社が定める追加的な責任又は権限を制限するものではない。
- 2. サイバーセキュリティ関連業務を管理し、実施し、又は検証する要員の責任、権限及び相互関係は、明確に定義され、文書化されなければならない。

3.2 トップマネジメントの責任

- 1. トップマネジメントは、CSMS の確立及び有効な実施について最終責任を負う。
- 2. トップマネジメントは、CSMS の有効な実施に必要な会社サイバーセキュリティ責任者その他の役割を任命しなければならない。

3.3 会社サイバーセキュリティ責任者

- 1. 会社サイバーセキュリティ責任者は、CSMS の有効な実施及び監督について全体的な責任を負う。
- 2. 当該責任者は、トップマネジメントに直接報告できる立場に置かれなければならない。
- 3. 当該責任者は、CSMS の有効な実施に必要な資源の確保について、トップマネジメントに対して要請する権限を有しなければならない。
- 4. 会社サイバーセキュリティ責任者の責任及び権限を定義し文書化しなければならない。当該責任及び権限には少なくとも次を含まなければならない。
 - (1) 会社及び管理船舶における CSMS の実施状況及び有効性の監視
 - (2) CSMS の実施状況に関するトップマネジメントへの報告
- 5. 会社は、会社サイバーセキュリティ責任者に対し、本ガイドラインに定めるもののほか、追加の責任又は権限を付与することができる。

3.4 船舶サイバーセキュリティ責任者

- 1. 船舶サイバーセキュリティ責任者は、各船舶における CSMS の運用について責任を負う。
- 2. 各船舶における船舶サイバーセキュリティ責任者の責任及び権限には、少なくとも次の事項を含まなければならない。
 - (1) 各船舶における CSMS の実施状況及び有効性の監視

(2) 各船舶における CSMS の実施状況の会社サイバーセキュリティ責任者への報告

3.5 船長の権限

会社は、CSMS の運用において、サイバーセキュリティ事象を含む船舶の安全及び環境保護に関する決定に対し、ISM コード A 部 5.2 に規定される船長の超越権限が適用されることを確保しなければならない。

4 章 経営資源及び能力に関する要求

本章は、CSMS の運用に必要な組織内部の資源及び要員の能力に関する要求を規定するものである。資源は、CSMS の構築から継続的改善に至る運用の全体を支える。なかでも CSMS を運用するのは人であり、役割に応じた能力の育成と組織全体の意識の向上が、その基盤となる。

4.1 資源の確保

- 1. 会社は、CSMS の確立、実施、維持及び継続的改善に必要な資源を決定し、これを提供しなければならない。
- 2. 当該資源には、本ガイドラインの適用範囲におけるサイバーリスクを管理するために必要な人的資源、技術的能力、財務的資源及び組織的支援を適宜含めるものとする。
- 3. 会社は、資源の決定に際し、3.3 に規定する会社サイバーセキュリティ責任者からの報告及び要請事項を考慮しなければならない。

4.2 能力

- 1. 会社は、3 章に基づき役割を任命された要員について、その責任及び権限に応じた必要な能力を定義しなければならない。
- 2. 会社は、当該役割を任命された要員が、定義された能力を満たしていることを確認しなければならない。
- 3. 能力は、適切な教育、訓練、経験又はそれらの組合せにより判断されなければならない。
- 4. 会社は、能力の証拠として、適切な文書化された情報を保持しなければならない。

4.3 教育及び訓練

- 1. 会社は、すべての従業員が次の事項を認識していることを確保しなければならない。
 - (1) サイバーセキュリティ方針
 - (2) CSMS マニュアル要求事項
 - (3) CSMS における自らの役割及び責任
 - (4) CSMS 要求事項を遵守しないことによる潜在的影響
- 2. 会社は、すべての従業員に対し、サイバーセキュリティに関する基本的な教育及び訓練を実施しなければならない。
- 3. 会社は、3 章に基づき役割を任命された要員に対し、その責任及び権限に応じた教育又は訓練を実施しなければならない。
- 4. 上記-2.及び-3.に規定する教育及び訓練は、12 か月を超えない期間で実施されなければならない。
- 5. 会社は、教育及び訓練の実施を裏付ける文書化された記録を保持しなければならない。

5章 サプライチェーンに関する要求

本章は、CSMS の運用に関わる組織外部の資源に対する管理を規定するものである。対象とするのは、CSMS の適用範囲に関連する請負者、供給者及びサービス提供者である。会社のサイバーリスク管理は、これらの者がサイバーセキュリティ上満たすべき要求を定め、それが満たされていることを確認するところまで及んで初めて完結する。

5.1 供給者への要求事項

- 1. CSMS の適用範囲に関連する場合、会社は、請負者、供給者及びサービス提供者（以下「供給者等」という。）が、その業務に関連して適用されるサイバーセキュリティ要求事項を認識し、これに適切に対応できることを確保しなければならない。
- 2. 会社は、供給者等に求める能力又は管理水準を定めなければならない。
- 3. 会社は、供給者等が前項の要求事項を満たしていることを確認し、その記録を保持しなければならない。

5.2 供給者の評価

会社は、CSMS に関連する業務を委託した供給者等が、**5.1** に規定する要求事項に適合していることを定期的に検証しなければならない。

6章 サイバーリスク評価に関する要求

本章は、サイバーリスクアセスメントの定義及び対象、並びに計画、実行及び見直しを含む実施プロセスを規定するものである。サイバーリスクアセスメントは、管理すべきサイバーリスクを把握し、適用する管理策を決定するための基礎となる。なお、本章は、リスク評価の手法を指定するものではない。

6.1 サイバーリスクアセスメントの役割

サイバーリスクアセスメントは、本ガイドラインに基づくサイバーセキュリティマネジメントの中核をなすものであり、船舶の IT 及び OT 環境に関連するサイバーリスクを特定し、評価し、その結果に基づき組織及び船舶に適した管理策を選択するための共通の意思決定プロセスである。

6.2 リスクアセスメントの対象

-1. サイバーリスクアセスメントは、対象となる船舶の安全運航、環境保護又は運航継続性に影響を及ぼし得る IT 及び OT システムを対象とする。これには船内システムを含むものとし、船内システムに直接接続し、または当該船舶の運航に影響を及ぼす陸上側システムも対象となり得る。

-2. 船内システムに接続せず、かつ、当該船舶の運航に影響を及ぼさない一般的な企業 IT システムは、原則としてリスクアセスメントの対象としない。

6.3 サイバーリスクアセスメントにおける実施プロセスの管理

-1. 会社は、サイバーリスクアセスメントの実施プロセスを文書化しなければならない。当該プロセスには、少なくとも以下を定めなければならない。

- (1) サイバーリスクアセスメントを実施する者
- (2) サイバーリスクアセスメントの結果をレビュー及び承認する者
- (3) 受容可能な残存リスクの考え方（定義）
- (4) 残存リスクを把握し、受容するか否かを判断する者
- (5) サイバーリスクアセスメントの見直しの方法

-2. 会社は、当該プロセスに基づきサイバーリスクアセスメントを実施し、当該プロセスが適用されたことを示す記録を保持しなければならない。

6.4 サイバーリスクの特定及び評価

-1. 会社は、サイバーリスクアセスメントの実施にあたり、**6.2**に規定する対象の IT／OT システム及びネットワーク構成を把握した上で、当該システム及び構成に関連するサイバーリスクを特定し、評価しなければならない。

-2. サイバーリスクの特定及び評価においては、少なくとも以下の要素を考慮しなければならない。

- (1) 当該 IT／OT 資産及びネットワーク構成に関連する脅威
- (2) 当該資産及び構成の状態又は特性により、リスクの原因となり得る要因（例：脆弱性、設定の不備、運用上の弱点）
- (3) 当該脅威が顕在化した場合の運航、安全、環境又は事業への影響

- (4) 当該脅威が発生する可能性
- (5) 船舶固有の運用条件（航行パターン、搭載貨物等）
- (6) 適用される法令，規則，契約上の要求事項その他の関連要求

-3. 会社は，サイバーリスクの評価結果に基づき，**8 章**に定める管理策のうちから適切なものを選択し，適用する範囲を定め，必要に応じて追加的対策を決定したうえで，これに適合するよう実装しなければならない。

-4. 会社は，第 8 章に定める管理策を実装しない場合，それにより残存するリスクを明確にし，その理由及び受容の判断を記録しなければならない。

-5. なお，本ガイドラインは，特定のリスク評価手法を規定するものではない。

6.5 サイバーリスクアセスメントの見直し

-1. 会社は，サイバーリスクアセスメントを，少なくとも 12 か月を超えない間隔で見直さなければならない。見直しの結果，必要と認めた場合には，サイバーリスクアセスメントを再実施しなければならない。

-2. **7 章**に規定する変更管理の対象となる変更が発生した場合，当該変更が影響を及ぼす範囲について，適切な時期にサイバーリスクアセスメントを再実施しなければならない。

7 章 構成管理に関する要求

本章は、6 章のリスクアセスメントの対象について、その構成管理を規定するものである。資産及びその運用環境の構成を維持し、管理することはサイバーリスク低減の出発点であり、本章は、特に変更が生じた場合の対応が確実に行われることを確保する。

7.1 構成管理

会社は、6 章のサイバーリスクアセスメントの対象となる IT/OT 資産及びネットワーク構成について、現在の構成及び変更履歴を管理しなければならない。

7.2 変更管理

会社は、IT/OT 資産、ネットワーク構成、ソフトウェア又は外部接続の変更を管理する手順を定めなければならない。当該手順には、変更在先立ち 6 章に定めるサイバーリスクアセスメントのプロセスに従いサイバーリスクを評価し、その結果に基づき 8 章に定める管理策の適用を見直した上で、変更を承認し、実施することを含めなければならない。

7.3 構成の見直し

会社は、構成及び設定が承認済みの状態を保っていることを定期的に確認しなければならない。

8 章 管理策

本章は、船舶の IT/OT システムに適用される管理策を分類して定めるものである。個別の管理策の選択は、6 章のリスクアセスメントの結果に基づき決定される。個別の管理策の内容は、第 2 部に示す。

8.a アクセス及び利用の管理

- 8.a.1 識別及び認証管理
- 8.a.2 認可及び特権管理
- 8.a.3 リモートアクセス及び第三者アクセスの管理
- 8.a.4 適切な利用及び利用者起因リスクの管理

8.b ネットワーク及び通信の保護

- 8.b.1 ネットワーク分離及びゾーニング
- 8.b.2 通信の保護
- 8.b.3 外部接続の管理

8.c システム構成及び保守

- 8.c.1 安全な構成及びハードニング
- 8.c.2 パッチ及び更新管理
- 8.c.3 陳腐化管理
- 8.c.4 マルウェア及びエンドポイント保護
- 8.c.5 ハードウェア及びソフトウェアの管理

8.d 媒体及び物理インターフェース管理

- 8.d.1 可搬媒体の管理
- 8.d.2 物理ポート及びインターフェースの保護
- 8.d.3 直接接続の管理
- 8.d.4 物理アクセスの管理

8.e 監視、ログ及び検知

- 8.e.1 イベントログ管理
- 8.e.2 セキュリティ監視
- 8.e.3 ログの保全及び保存
- 8.e.4 ログのレビュー及び異常調査

8.f バックアップ及び復旧

- 8.f.1 バックアップ方針及び実施
- 8.f.2 復旧手順
- 8.f.3 バックアップ及び復旧手順の検証

9 章 緊急事態対応に関する要求

本章は、緊急事態対応に関する要求を規定するものである。CSMS の運用において報告すべき事象を定義したうえで、船舶と陸上が連携して対応するための報告の経路と内容を、必要に応じて第三者専門家等への連絡を含めて確立し、更に定期的な操練を実施することで緊急事態に備えることを求めるものである。

9.1 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サイバーインシデント及びそれに起因する緊急事態を識別し、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。

9.2 緊急事態への対応プログラムの確立

会社は、サイバーインシデント及びそれに起因する緊急事態への対応に備えるため、操練のプログラムを確立しなければならない。

9.3 緊急事態への対応を確保する手段の提供

会社は、サイバーインシデントへの対応に必要な支援を平時から確保しなければならない。

10 章 不適合及び是正措置に関する要求

本章は、CSMS の運用を通じて識別された不適合の取扱いを規定するものである。不適合は、継続的改善のため、原因の調査、対応及び是正措置の対象となる。

10.1 不適合の報告及び分析

会社は、不適合が会社に報告され、CSMS の有効性の向上を目的として調査及び分析されることを確保する手順を確立しなければならない。

10.2 是正措置及び再発防止策

会社は、再発防止策を含む是正措置を実施するための手順を確立しなければならない。

11 章 文書管理に関する要求

本章は、CSMS に関する文書の管理を規定するものである。当該文書の作成、改訂及び廃止は、本章に基づき定められた文書管理手順により管理される。

11.1 文書管理手順の確立及び維持

-1. 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。

-2. 前-1.の文書管理手順においては、少なくとも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確認されており、承認されていること、及び
- (3) 廃止文書はすみやかに取り除かれていること。

11.2 サイバーセキュリティマネジメントマニュアル

会社は、CSMS を記述する文書を「サイバーセキュリティマネジメントマニュアル」として作成し、会社の公式文書として維持しなければならない。当該マニュアルは、会社に適用される文書及び各対象船舶に適用される文書から構成される。文書化の様式は、会社が最も効果的と判断するものとすることができる。会社は、各船舶に、本船に適用される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，見直し及び評価に関する要求

本章は，CSMS の継続的改善を目的として，内部監査及びトップマネジメントによるレビューを通じた CSMS の運用の見直しを規定するものである。

12.1 内部サイバーセキュリティ監査

- 1. 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，会社及び船舶に対し 12 か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。
- 2. 監査を行う者は，被監査部署から独立し，かつ，サイバーセキュリティに関する監査を適切に実施するために必要な力量を有していなければならない。
- 3. 会社は監査の結果を関係する部署の責任者に周知しなければならない。監査において摘出された不適合は，10 章に定める是正措置の手順に従い処理しなければならない。

12.2 サイバーセキュリティマネジメントシステムの評価

トップマネジメントは，CSMS の有効性を定期的に見直さなければならない。会社は，見直しの結果を関係する部署の責任者に周知しなければならない。

第 2 部 評価基準及び客観的証拠

第 2 部は、第 1 部に定める要求事項及び管理策について、本会の審査における評価基準及び求められる客観的証拠を示すものである。

第 1 部が会社の構築すべき CSMS の要求事項を定めるのに対し、第 2 部は、会社が当該要求事項を確立し、実施し、維持していることを本会が審査する際の基準と、その際に確認する客観的証拠を、要求事項ごとに示す。会社は、これらを参照することにより、各要求事項について何を整備し、審査において何が確認されるのかを把握することができる。

第 1 部第 8 章に掲げる各管理策については、その実装において満たすべき事項を、評価基準として具体的に示す。これらの評価基準は、特定の技術的解決策又は製品を要求するものではない。会社は、サイバーリスクアセスメントの結果、船舶の特性、運航形態及び適用される外部要求事項を踏まえ、適切な管理策を決定し、実施する。

1 章 適用範囲及び基本要求

1.1 サイバーセキュリティマネジメントの目的

対応する第 1 部の要求事項

サイバーセキュリティマネジメントの目的は、会社が、船舶運航におけるサイバーリスクを体系的に評価・管理し、運航の安全性、環境保護及び運航継続性を確保することにある。

評価基準

本項単独では評価せず、以降の各項により評価する。

求められる客観的証拠

本項単独では評価せず、以降の各項により評価する。

外部要件の対応

—

1.2 サイバーセキュリティマネジメントシステム（CSMS）の目的

対応する第 1 部の要求事項

サイバーセキュリティマネジメントシステム（CSMS）の目的は、会社が船舶のサイバーセキュリティマネジメントを運用するための仕組みを構築し、次の事項を達成することにある。

- 1. 船舶の IT 及び OT システムに関連するサイバーリスクを識別し、評価すること。
- 2. 評価されたサイバーリスクに対し、適切な管理策を決定し実施すること。
- 3. サイバーインシデントへの対応及び復旧並びに緊急事態への準備を確保すること。
- 4. 会社及び船舶におけるマネジメントの有効性を継続的に改善すること。

評価基準

本項単独では評価せず、以降の各項により評価する。

求められる客観的証拠

本項単独では評価せず、以降の各項により評価する。

外部要件の対応

—

1.3 関連する規則、条約、コード及び指針との両立性

対応する第 1 部の要求事項

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
- 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。

評価基準

CSMS マニュアルにおいて、適用される法令、条約又は関連指針が参照されている。

求められる客観的証拠

CSMS マニュアル

外部要件の対応

—

1.4 適用

対応する第 1 部の要求事項

本ガイドラインは、会社及び当該会社が適用対象とする船舶に適用する。

評価基準

CSMS マニュアルにおいて、適用対象となる船舶、IT 及び OT システム、並びに船舶運航に影響を及ぼす陸上システムの範囲が明確に定義されている。

求められる客観的証拠

CSMS マニュアル、リスク評価文書等（CSMS の適用範囲又はリスク評価の範囲が規定されていることを確認するための文書）

外部要件の対応

- ・ DryBMS (No. 28) : Excellence
- ・ TMSA 3 (Element 13) : Stage 1, 13.1.1
- ・ MSC-FAL.1/Circ.3/Rev.3 : 2.3.1
- ・ IACS Rec. 194 : 3.2, 3.3

1.5 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

対応する第 1 部の要求事項

会社は、次の事項を含む 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. リスクアセスメントの実施手順
- 3. 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
- 4. 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
- 5. 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
- 6. 緊急事態に対する準備及び対応の手順書
- 7. 内部監査及び経営者による見直しに関する手順書

評価基準

CSMS マニュアルにおいて、第 1 部 1.3-1～-7 に示される要素が規定されている。

求められる客観的証拠

CSMS マニュアル

外部要件の対応

- ・ DryBMS (No. 28) : Basic
- ・ SIRE 2.0 : Section 7.5

- TMSA 3 (Element 13) : Stage 1, 13.1, 13.1.1

ClassNK

2 章 リーダーシップ及び方針に関する要求

2.1 サイバーセキュリティ方針の確立

対応する第 1 部の要求事項

会社は、1.2 の目的を達成する方策を含む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。

評価基準

サイバーセキュリティ方針が文書化されており、1.2 に定める目的を達成するための方策（船舶運航におけるサイバーリスク管理に対する会社の取組方針）が方針に示されている。

方針はトップマネジメントにより正式に承認されており、コミットメントを示す証拠（署名又はそれに相当する承認記録等）が存在する。

方針は少なくとも次の内容を含んでいる。

- ・ 1.2 に定める目的を達成するための方策が方針に示されていること。
- ・ 会社としてのコミットメントが示されていること。

求められる客観的証拠

サイバーセキュリティ方針の文書が存在し、少なくとも次が確認できること。

- ・ 1.2 に定める目的を達成するための方策（船舶運航におけるサイバーリスク管理に対する会社の取組方針）が方針に記載されていること。
- ・ 会社としてのコミットメントが示されていること。

トップマネジメントによる承認の証拠が存在し、少なくとも次が確認できること。

- ・ 方針がトップマネジメントにより正式に承認されていること（例：署名、承認者及び承認日が記録された承認記録等）。

外部要件の対応

- ・ RISQ v3.2 : 12.7
- ・ DryBMS (No. 28) : Basic
- ・ TMSA 3 (Element 13) : Stage 2, 13.2.3, 13.3.3
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.3, 3.5.1

2.2 サイバーセキュリティ方針の実施及び維持

対応する第 1 部の要求事項

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。

評価基準

方針が陸上及び船上の組織のすべての階層において実施されており、関連する要員に周知されている。

方針が、12.2 に定める見直しその他の機会における定期的な見直し及び更新を通じて最新の状態に維持されている。

求められる客観的証拠

方針が関連要員に周知されていることを示す証拠が存在し、少なくとも以下が確認でき

ること。

- ・方針又はその参照先が，陸上及び船上の関連要員がアクセスできる状態にあること。
- ・教育記録，習熟記録又は同等の記録により，関連要員が方針の内容及び要求事項について周知されていることが確認できること。

方針が最新の状態に維持されていることを示す証拠が存在し，少なくとも以下が確認できること。

- ・定期的な見直しの記録が存在すること（例：マネジメントレビュー議事録，改訂履歴等）。

外部要件の対応

—

3 章 統治体制及び責任に関する要求

3.1 役割及び責任

対応する第 1 部の要求事項

- 1. 会社は、CSMS の有効な実施に必要な役割及び責任を特定し、定義し、文書化しなければならない。これには、本章に規定する会社サイバーセキュリティ責任者及び船舶サイバーセキュリティ責任者を含むが、これらに限定されない。本ガイドラインに定める責任は最低限の要求事項であり、会社が定める追加的な責任又は権限を制限するものではない。
- 2. サイバーセキュリティ関連業務を管理し、実施し、又は検証する要員の責任、権限及び相互関係は、明確に定義され、文書化されなければならない。

評価基準

- 1. CSMS の有効な実施に必要なすべての役割及び責任が特定、定義及び文書化されており、少なくとも会社サイバーセキュリティ責任者及び船舶サイバーセキュリティ責任者を含むこと。
- 2. 以下を満たすこと。
 - ・サイバーセキュリティ関連業務を管理、実施又は検証するすべての要員の責任、権限及び相互関係が明確に定義され文書化されていること。
 - ・本社・船舶間のインターフェースが文書化された体制に含まれていること。
 - ・外部要求事項上特に責任の所在が問われる役割（例：船内ネットワークにおけるユーザープロファイル及びパスワード管理の責任者）が特定されていること。

求められる客観的証拠

- 文書化された CSMS 組織体制が存在し、少なくとも以下が確認できること。
 - ・会社組織図及びサイバーセキュリティ体制図等により、CSMS の有効な実施に必要な役割が特定されており、少なくとも会社サイバーセキュリティ責任者及び船舶サイバーセキュリティ責任者、並びに会社が設けた追加的な役割が示されていること。
 - ・船内ネットワークにおけるユーザープロファイル及びパスワード管理の責任者が特定されていること。
- 手順書その他の CSMS 文書において、サイバーセキュリティ関連の役割ごとに、少なくとも以下が確認できること。
 - ・各役割の責任、権限及び相互関係が記述されていること。
 - ・本社・船上要員間のインターフェースが取り扱われていること。

外部要件の対応

- ・ DryBMS (No. 28) : Basic
- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : 13.1.1
- ・ IACS Rec. 194 : RESPOND, Item 11

3.2 トップマネジメントの責任

対応する第 1 部の要求事項

- 1. トップマネジメントは、CSMS の確立及び有効な実施について最終責任を負う。

-2. トップマネジメントは、CSMS の有効な実施に必要な会社サイバーセキュリティ責任者その他の役割を任命しなければならない。

評価基準

-1. トップマネジメントが CSMS の確立及び有効な実施について最終責任を負っており、その責任がサイバーセキュリティ方針の承認（2.1）等を通じて示されていることが確認できること。

-2. トップマネジメントが、CSMS の有効な実施に必要な役割（少なくとも会社サイバーセキュリティ責任者を含む）の任命について責任を負い、当該役割が任命されていることが確認できること。

求められる客観的証拠

トップマネジメントの CSMS に対する最終責任を示す証拠が存在し、少なくとも以下が確認できること。

- ・任命に少なくとも会社サイバーセキュリティ責任者が含まれていること。

- ・トップマネジメントがサイバーセキュリティ方針を承認・署名していること（2.1 参照）。これをもって CSMS に対する最終責任が示されていること。

CSMS の有効な実施に必要な役割の任命に関する証拠が存在し、少なくとも以下が確認できること。

- ・トップマネジメントの責任の下で、CSMS の有効な実施に必要な役割が任命されていること（例：任命文書、CSMS マニュアル中の任命に関する記述、職位指定又は任命権限の委譲に関する記述等）。

外部要件の対応

—

3.3 会社サイバーセキュリティ責任者

対応する第 1 部の要求事項

-1. 会社サイバーセキュリティ責任者は、CSMS の有効な実施及び監督について全体的な責任を負う。

-2. 当該責任者は、トップマネジメントに直接報告できる立場に置かれなければならない。

-3. 当該責任者は、CSMS の有効な実施に必要な資源の確保について、トップマネジメントに対して要請する権限を有しなければならない。

-4. 会社サイバーセキュリティ責任者の責任及び権限を定義し文書化しなければならない。当該責任及び権限には少なくとも次を含まなければならない。

- (1) 会社及び管理船舶における CSMS の実施状況及び有効性の監視

- (2) CSMS の実施状況に関するトップマネジメントへの報告

-5. 会社は、会社サイバーセキュリティ責任者に対し、本ガイドラインに定めるもののほか、追加の責任又は権限を付与することができる。

評価基準

-1. 会社サイバーセキュリティ責任者が、CSMS の有効な実施及び監督について全体的な責任を負う者として位置づけられていることが確認できること。

-2. 会社サイバーセキュリティ責任者が、トップマネジメントに直接報告できる立場に

置かれていることが確認できること。

-3. 会社サイバーセキュリティ責任者が、CSMS の有効な実施に必要な資源の確保についてトップマネジメントに要請する権限を有していることが確認できること。

-4. 会社サイバーセキュリティ責任者の責任及び権限が定義され文書化されており、少なくとも次を含むこと。

(1) 会社及び対象船における CSMS の実施状況及び有効性の監視

(2) CSMS の実施状況に関するトップマネジメントへの報告

求められる客観的証拠

会社サイバーセキュリティ責任者の責任及び権限を定める文書（CSMS マニュアル等）が存在し、少なくとも以下が確認できること。

・会社サイバーセキュリティ責任者が、CSMS の有効な実施及び監督について全体的な責任を負う者として記述されていること。

・責任及び権限に、CSMS の実施状況及び有効性の監視並びにトップマネジメントへの報告が含まれていること。

・CSMS の有効な実施に必要な資源の確保についてトップマネジメントに要請する権限が記述されていること。

組織体制において、会社サイバーセキュリティ責任者からトップマネジメントへの直接報告関係が確認できること。

・組織図又は報告経路の記述により、トップマネジメントへの直接報告が示されていること。

外部要件の対応

- ・ DryBMS (No. 28) : Basic
- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : 13.1.4
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.1, 3.5.1.2
- ・ IACS Rec. 194 : RESPOND, Item 11

3.4 船舶サイバーセキュリティ責任者

対応する第 1 部の要求事項

-1. 船舶サイバーセキュリティ責任者は、各船舶における CSMS の運用について責任を負う。

-2. 各船舶における船舶サイバーセキュリティ責任者の責任及び権限には、少なくとも次の事項を含まなければならない。

(1) 各船舶における CSMS の実施状況及び有効性の監視

(2) 各船舶における CSMS の実施状況の CSMS 運用責任者への報告

評価基準

-1. 船舶サイバーセキュリティ責任者が、各船舶における CSMS の運用について責任を負う者として位置づけられていることが確認できること。

-2. 船舶サイバーセキュリティ責任者の責任及び権限が、少なくとも次を含むこと。

(1) 各船舶における CSMS の実施状況及び有効性の監視

(2) 各船舶における CSMS の実施状況の会社サイバーセキュリティ責任者への報告

求められる客観的証拠

適用対象の各船舶について、船舶サイバーセキュリティ責任者の責任及び権限を定める文書（CSMS マニュアル等）が存在し、少なくとも以下が確認できること。

- ・各船舶において船舶サイバーセキュリティ責任者が氏名又は役職により特定されていること。
- ・その責任及び権限に、各船舶における CSMS の実施状況及び有効性の監視並びに会社サイバーセキュリティ責任者への報告が含まれていること。

外部要件の対応

- ・ DryBMS（No. 28）：Basic
- ・ SIRE 2.0：Section 7.5
- ・ MSC-FAL.1/Circ.3/Rev.3：3.5.1, 3.5.1.2

3.5 船長の権限

対応する第 1 部の要求事項

会社は、CSMS の運用において、サイバーセキュリティ事象を含む船舶の安全及び環境保護に関する決定に対し、ISM コード A 部 5.2 に規定される船長の超越権限が適用されることを確保しなければならない。

評価基準

CSMS の文書において、ISM コード A 部 5.2 に基づく船長の超越権限が保全されており、サイバーセキュリティ事象を含む船舶の安全及び環境保護に関する決定に適用されることが明記されていること。

求められる客観的証拠

CSMS マニュアル又は同等の文書に、次が確認できること。

- ・船長の超越権限に関する記述があり、ISM コード A 部 5.2 を参照し、又はこれと整合していること。
- ・当該権限がサイバーセキュリティ事象に関する決定にも及ぶことが示されていること。

外部要件の対応

—

4 章 経営資源及び能力に関する要求

4.1 資源の確保

対応する第 1 部の要求事項

- 1. 会社は、CSMS の確立、実施、維持及び継続的改善に必要な資源を決定し、これを提供しなければならない。
- 2. 当該資源には、本ガイドラインの適用範囲におけるサイバーリスクを管理するために必要な人的資源、技術的能力、財務的資源及び組織的支援を適宜含めるものとする。
- 3. 会社は、資源の決定に際し、3.3 に規定する会社サイバーセキュリティ責任者からの報告及び要請事項を考慮しなければならない。

評価基準

会社サイバーセキュリティ責任者が、マネジメントレビュー等の決まった機会を含め、資源に関する報告又は要請を述べる機会を与えられており、会社がこれを検討するプロセスが存在すること。

注：本項の評価は、会社が資源に関する報告又は要請を検討する仕組みの有無を対象とし、どのような資源をどれだけ提供するかという会社の判断結果そのものは評価しない。

求められる客観的証拠

会社サイバーセキュリティ責任者が資源に関する意見を述べ、会社が検討する仕組みが確認できること。

- ・ マネジメントレビュー等の決まった機会において、会社サイバーセキュリティ責任者が資源に関する報告又は要請を行う機会が設けられていること（例：マネジメントレビュー議事録、会議体の規程等）。
- ・ 提起された資源に関する報告又は要請が、会社において検討された記録が存在すること（例：議事録等）。

外部要件の対応

- ・ MSC-FAL.1/Circ.3/Rev.3 : 2.3.2

4.2 能力

対応する第 1 部の要求事項

- 1. 会社は、3 章に基づき役割を任命された要員について、その責任及び権限に応じた必要な能力を定義しなければならない。
- 2. 会社は、当該役割を任命された要員が、定義された能力を満たしていることを確認しなければならない。
- 3. 能力は、適切な教育、訓練、経験又はそれらの組合せにより判断されなければならない。
- 4. 会社は、能力の証拠として、適切な文書化された情報を保持しなければならない。

評価基準

- 1. 3 章に基づき任命された各役割について、その責任及び権限に応じた必要な能力が定義されていること。
- 2. 当該役割を任命された要員が、定義された能力を満たしていることを会社が確認し

ていること。

- 3. 能力が、適切な教育、訓練、経験又はそれらの組合せにより判断されていること。
- 4. 能力の証拠として、文書化された情報が保持されていること。

求められる客観的証拠

役割ごとの能力要件を定めた文書（職務記述、力量要件表、CSMS マニュアル記述等）が存在し、少なくとも以下が確認できること。

- ・会社サイバーセキュリティ責任者について、その職務遂行に必要な知識・経験（例：サイバーリスク管理、海事 IT/OT、関連規格・外部要求の理解等）が、要件として具体的に示されていること。
- ・船舶サイバーセキュリティ責任者その他の役割について、それぞれの責任に応じた必要な知識・技能が示されていること。

各要員が能力要件を満たすことを示す記録が存在し、少なくとも以下が確認できること。

- ・各要員について、定義された能力要件のそれぞれが、いずれの手段（教育・訓練・経験又はその組合せ）で満たされているかが、記録により確認できること（例：研修修了証、資格、業務経歴、力量評価記録等）。
- ・要件と実績が突き合わせられており、要件に対して充足が確認されていること（要件と保有能力の対応が辿れること）。

外部要件の対応

- ・ DryBMS (No. 28) : Basic
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.1, 3.5.2
- ・ IACS Rec. 194 : PROTECT, Item 9

4.3 教育及び訓練

対応する第1部の要求事項

- 1. 会社は、すべての従業員が次の事項を認識していることを確保しなければならない。
 - (1) サイバーセキュリティ方針
 - (2) CSMS マニュアル要求事項
 - (3) CSMS における自らの役割及び責任
 - (4) CSMS 要求事項を遵守しないことによる潜在的影響
- 2. 会社は、すべての従業員に対し、サイバーセキュリティに関する基本的な教育及び訓練を実施しなければならない。
- 3. 会社は、**3章**に基づき役割を任命された要員に対し、その責任及び権限に応じた教育又は訓練を実施しなければならない。
- 4. 上記**-2.**及び**-3.**に規定する教育及び訓練は、12 か月を超えない期間で実施されなければならない。
- 5. 会社は、教育及び訓練の実施を裏付ける文書化された記録を保持しなければならない。

評価基準

- 1. すべての従業員が、次の事項を認識していることが確保されていること。
 - (1) サイバーセキュリティ方針
 - (2) CSMS マニュアル要求事項
 - (3) CSMS における自らの役割及び責任

(4) CSMS 要求事項を遵守しないことによる潜在的影響

-2. 以下を満たすこと。

- ・すべての従業員に対し、サイバーセキュリティに関する基本的な教育及び訓練が実施されていること。
- ・外部要求事項上求められる教育及び意識向上に関する取組が講じられていること（例：基本的な訓練へのサイバーインシデントの対応及び復旧に関する内容の包含、ポスター・CBT・オンラインコース等を用いた船内での意識向上の積極的な推進、乗組員交代時を含む習熟プロセスの一環としてのセキュリティブリーフィングの実施）。

-3. 以下を満たすこと。

- ・**3 章**に基づき役割を任命された要員に対し、その責任及び権限に応じた教育又は訓練が実施されていること。
- ・当該要員が、自らの責任に係る会社のサイバーリスク管理手順を理解していること。

-4. 上記-2.及び-3.に定める教育及び訓練が、12 か月を超えない期間で実施されていること。

-5. 教育及び訓練の実施を裏付ける文書化された記録が保持されていること。

求められる客観的証拠

全従業員に対する教育及び訓練の記録が存在し、少なくとも以下が確認できること。

- ・全従業員に基本的なサイバーセキュリティ教育及び訓練が実施され、内容が方針、CSMS 要求事項、自らの役割及び責任、不遵守による潜在的影響を扱っていること。
- ・実施間隔が 12 か月を超えていないこと（実施日の記録により確認できること）。
- ・外部要求事項上求められる教育及び意識向上に関する取組が確認できること（例：基本的な訓練にサイバーインシデントの対応及び復旧に関する内容が含まれていること、船内で意識向上の手段が用いられていること（ポスター・CBT・オンラインコース等）、乗組員交代時を含む習熟プロセスの一環としてセキュリティブリーフィングが実施されていること）。

3 章に基づく役割保有者に対する役割別教育の記録が存在し、かつ当該要員の理解が確認できること。

- ・教育又は訓練の内容が、当該役割の責任及び権限に応じたものであること。
- ・実施日及び受講（修了）が記録されていること。
- ・サイバーリスク管理実施に責任のある要員等への面談により、自らの責任に係る会社のサイバーリスク管理手順（航行・推進に重要な OT システムのバックアップ体制を含む）を理解していることが確認できること。

外部要件の対応

- ・DryBMS（No. 28）：Basic
- ・SIRE 2.0：Section 7.5
- ・TMSA 3（Element 13）：Stage 1, 13.1.3
- ・MSC-FAL.1/Circ.3/Rev.3：3.5.3.6, 3.5.4.2, 3.5.5.3, 3.5.6.2, 3.7

5 章 サプライチェーンに関する要求

5.1 供給者への要求事項

対応する第 1 部の要求事項

- 1. CSMS の適用範囲に関連する場合、会社は、請負者、供給者及びサービス提供者（以下「供給者等」という。）が、その業務に関連して適用されるサイバーセキュリティ要求事項を認識し、これに適切に対応できることを確保しなければならない。
- 2. 会社は、供給者等に求める能力又は管理水準を定めなければならない。
- 3. 会社は、供給者等が前項の要求事項を満たしていることを確認し、その記録を保持しなければならない。

評価基準

- 1. CSMS の適用範囲に関連する場合、供給者等が、その業務に関連して適用されるサイバーセキュリティ要求事項を認識し、これに適切に対応できることが確保されていること。
- 2. 供給者等に求める能力又は管理水準が定義されていること。
- 3. 以下を満たすこと。
 - ・供給者等が上記-2.に定める要求事項を満たしていることを会社が確認し、その記録を保持していること。
 - ・外部要求事項上求められる供給者管理に関する事項が講じられていること（例：脅威緩和のために用いる独立した専門家支援に係る契約前のデューデリジェンス評価及び業務範囲の明確化、システムへのアクセス許可に先立つ信用調査又は独立監査人報告書の活用）。

求められる客観的証拠

CSMS の適用範囲に関連する供給者等への要求事項を定めた文書が存在し、少なくとも以下が確認できること。

- ・供給者等が認識し又は遵守すべき適用可能なサイバーセキュリティ要求事項が特定されていること。
 - ・供給者等に求める能力又は管理水準が定義されていること。
- 供給者等の確認記録が存在し、少なくとも以下が確認できること。
- ・関連する供給者等が適用可能な要求事項について通知されていることを示す証拠が存在すること（例：契約条項、連絡記録、事前評価記録等）。
 - ・要求事項の充足が確認され、その記録が保持されていること。
 - ・外部要求事項上求められる供給者管理に関する事項が確認できること（例：独立した専門家支援に係る契約前のデューデリジェンス評価及び業務範囲の明確化、システムへのアクセス許可に先立つ信用調査又は独立監査人報告書の活用）。

外部要件の対応

- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.8
- ・ IACS Rec. 194 : PROTECT, Item 9

5.2 供給者の評価

対応する第1部の要求事項

会社は、CSMSに関連する業務を委託した供給者等が、5.1に規定する要求事項に適合していることを定期的に検証しなければならない。

評価基準

- ・ CSMSに関連する業務を委託した供給者等が、5.1に規定する要求事項（5.1において会社が定めた能力又は管理水準を含む）に適合していることが、会社が定めた周期又はタイミングで検証されていること。
- ・ 検証の結果、要求事項を満たしていないことが判明した場合は、10章に基づき規定された不適合処理手順に従うことが規定されていること。

求められる客観的証拠

供給者等の評価に関する手順及び記録が存在し、少なくとも以下が確認できること。

- ・ 供給者等の評価を行う周期又はタイミングが会社により定められていること。
- ・ CSMSに関連する業務を委託した供給者等について、5.1で会社が定めた要求事項（能力又は管理水準）への適合状況が、当該周期又はタイミングで検証され、その結果が記録されていること。
- ・ 検証により要求事項を満たしていないことが判明した場合は10章に基づく手順により処理することが規定されており、該当事例がある場合は当該手順により処理されていること。当該処理の結果として取られる対応には、例えば、供給者等への是正要求、供給者等のポリシー又は手順の更新要請、契約の見直し、供給者等の変更等が含まれる。

外部要件の対応

—

6 章 サイバーリスク評価に関する要求

6.1 サイバーリスクアセスメントの役割

対応する第 1 部の要求事項

サイバーリスクアセスメントは、本ガイドラインに基づくサイバーセキュリティマネジメントの中核をなすものであり、船舶の IT 及び OT 環境に関連するサイバーリスクを特定し、評価し、その結果に基づき組織及び船舶に適した管理策を選択するための共通の意思決定プロセスである。

評価基準

本項単独では評価せず、以降の各項により評価する。

求められる客観的証拠

本項単独では評価せず、以降の各項により評価する。

外部要件の対応

—

6.2 サイバーリスクアセスメントの対象

対応する第 1 部の要求事項

-1. サイバーリスクアセスメントは、対象となる船舶の安全運航、環境保護又は運航継続性に影響を及ぼし得る IT 及び OT システムを対象とする。これには船内システムを含むものとし、船内システムに直接接続し、または当該船舶の運航に影響を及ぼす陸上側システムも対象となり得る。

-2. 船内システムに接続せず、かつ、当該船舶の運航に影響を及ぼさない一般的な企業 IT システムは、原則としてリスクアセスメントの対象としない。

評価基準

本項単独では評価せず、以降の各項により評価する。

求められる客観的証拠

本項単独では評価せず、以降の各項により評価する。

外部要件の対応

—

6.3 サイバーリスクアセスメントにおける実施プロセスの管理

対応する第 1 部の要求事項

-1. 会社は、サイバーリスクアセスメントの実施プロセスを文書化しなければならない。当該プロセスには、少なくとも以下を定めなければならない。

- (1) サイバーリスクアセスメントを実施する者
- (2) サイバーリスクアセスメントの結果をレビュー及び承認する者
- (3) 受容可能な残存リスクの考え方（定義）
- (4) 残存リスクを把握し、受容するか否かを判断する者

(5) サイバーリスクアセスメントの見直しの方法

-2. 会社は、当該プロセスに基づきサイバーリスクアセスメントを実施し、当該プロセスが適用されたことを示す記録を保持しなければならない。

評価基準

-1. サイバーリスクアセスメントの実施プロセスが文書化されており、少なくとも次が定められていること。

- (1) 実施する者
- (2) 結果をレビュー及び承認する者
- (3) 受容可能な残存リスクの考え方（定義）
- (4) 残存リスクを把握し、受容するか否かを判断する者
- (5) 見直しの方法

-2. 当該プロセスに基づきサイバーリスクアセスメントが実施され、当該プロセスが適用されたことを示す記録が保持されていること。

求められる客観的証拠

文書化されたサイバーリスクアセスメントのプロセスが存在し、少なくとも以下が確認できること。

- ・ 6.3-1 に定める 5 要素が定められていること。

完了したアセスメントの記録が存在し、少なくとも以下が確認できること。

- ・ 指定された者によるレビュー及び承認が実施されていること。
- ・ 残存リスクが特定され、受容の判断が記録されていること。

外部要件の対応

- ・ DryBMS（No. 28）：Basic
- ・ SIRE 2.0：Section 7.5
- ・ TMSA 3（Element 13）：Stage 2, 13.2.1
- ・ MSC-FAL.1/Circ.3/Rev.3：3.5.3

6.4 サイバーリスクの特定及び評価

対応する第 1 部の要求事項

-1. 会社は、サイバーリスクアセスメントの実施にあたり、6.2 に規定する対象の IT/OT システム及びネットワーク構成を把握した上で、当該システム及び構成に関連するサイバーリスクを特定し、評価しなければならない。

-2. サイバーリスクの特定及び評価においては、少なくとも以下の要素を考慮しなければならない。

- (1) 当該 IT/OT 資産及びネットワーク構成に関連する脅威
- (2) 当該資産及び構成の状態又は特性により、リスクの原因となり得る要因（例：脆弱性、設定の不備、運用上の弱点）
- (3) 当該脅威が顕在化した場合の運航、安全、環境又は事業への影響
- (4) 当該脅威が発生する可能性
- (5) 船舶固有の運用条件（航行パターン、搭載貨物等）
- (6) 適用される法令、規則、契約上の要求事項その他の関連要求

-3. 会社は、サイバーリスクの評価結果に基づき、8 章に定める管理策のうちから適切なものを選択し、適用する範囲を定め、必要に応じて追加的対策を決定したうえで、これに

適合するよう実装しなければならない。

-4. 会社は、**8章**に定める管理策を実装しない場合、それにより残存するリスクを明確にし、その理由及び受容の判断を記録しなければならない。

-5. なお、本ガイドラインは、特定のリスク評価手法を規定するものではない。

評価基準

-1. **6.2**に規定する対象のIT/OTシステム及びネットワーク構成を把握した上で、当該システム及び構成に関連するサイバーリスクが特定され、評価されていること。

-2. サイバーリスクの特定及び評価において、**6.4-2**に定める要素が考慮されていること。

-3. 評価結果に基づき、**8章**に定める管理策のうちから適切なものが選択され、適用する範囲が定められ、必要に応じて追加的対策が決定されたうえで、これに適合するよう実装されていること。

-4. 管理策を実装しない場合に、それにより残存するリスクが明確にされ、その理由及び受容の判断が記録されていること。

求められる客観的証拠

船内IT/OT資産一覧（対象機器・システム一覧等）が存在し、各システムについて少なくとも以下が把握できること。**6.2**により陸上側システムを対象とする場合は、当該システムも対象に含める。

- ・ 機器種別、製造者、ソフトウェアバージョン及びパッチ更新状況
- ・ 一覧に少なくとも次のシステムが含まれていること（搭載されている場合）：貨物管理システム、ブリッジシステム、推進・機関管理及び電力制御システム、アクセス制御システム、事務・乗組員福祉システム、通信システム。
- ・ 当該資産一覧が維持・更新されていること（例：最終更新日の確認等）。

ネットワーク構成図（システム・ネットワーク構成図等）が存在し、少なくとも以下が確認できること。

- ・ ゾーンの区分及び名称が定義されていること。
- ・ ゾーン間の接続関係及び外部接続点が示されていること。

完了したサイバーリスクアセスメントの記録が存在し、少なくとも以下が確認できること。

- ・ **6.4-2**に定める要素が取り扱われており、外部及び内部の脅威の両方の識別が含まれていること。
- ・ 当該船舶の航行海域に適用される脅威が取り扱われていること。
- ・ 評価結果に基づき選択された管理策及び受容された残存リスクが、根拠とともに文書化されていること。
- ・ 脆弱性が悪用される可能性及び悪用された場合の影響の両方を低減する観点が反映されていること。

外部要件の対応

- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 1, Stage 2, Stage 4, 13.1.2, 13.1.5, 13.1.3, 13.2.1, 13.2.3, 13.4.1
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.4, 3.5, 3.5.2, 3.5.2.1, 3.5.2.2, 3.5.2.3
- ・ IACS Rec. 194 : IDENTIFY, PROTECT, DETECT, RECOVER, Item 1, Item 2, Item 3, Item 4, Item 5, Item 6, Item 7, Item 10, Item 13

6.5 サイバーリスクアセスメントの見直し

対応する第1部の要求事項

- 1. 会社は、サイバーリスクアセスメントを、少なくとも12か月を超えない間隔で見直さなければならない。見直しの結果、必要と認めた場合には、サイバーリスクアセスメントを再実施しなければならない。
- 2. 7章に規定する変更管理の対象となる変更が発生した場合、当該変更が影響を及ぼす範囲について、適切な時期にサイバーリスクアセスメントを再実施しなければならない。

評価基準

- 1. サイバーリスクアセスメントが、12か月を超えない間隔で見直されており、見直しの結果必要と認めた場合には再実施されていること。
- 2. 7章に規定する変更管理の対象となる変更が発生した場合、当該変更が影響を及ぼす範囲について、適切な時期に再実施されていること。
- 3. 適切な外部情報源（例：業界アドバイザリー、旗国ガイダンス、船級協会ガイドライン等）から最新のセキュリティ関連情報を入手する仕組みが存在し、入手した情報が見直され、関連する場合にサイバーリスクアセスメント又は手順に反映されていること。

求められる客観的証拠

サイバーリスクアセスメントの見直し記録が存在し、少なくとも以下が確認できること。

- ・直近の見直し日が前回から12か月を超えていないこと。
- ・見直しの結果（再実施の要否の判断を含む）が記録されていること。
- ・7章の変更管理の対象となる変更が発生した場合、当該変更に伴う再実施が行われていること。

外部情報の入手及び反映に関する手順又は記録が存在し、少なくとも以下が確認できること。

- ・適切な外部情報源から最新のセキュリティ関連情報を入手する仕組みが存在すること（例：業界アドバイザリー、旗国ガイダンス、船級協会ガイドライン等）。
- ・入手した情報が見直され、関連する場合にリスクアセスメント又は手順の更新に反映されていることを示す記録が存在すること。

外部要件の対応

- ・TMSA 3（Element 13）：Stage 1, Stage 2, Stage 3, 13.1.4, 13.2.1, 13.3.2

7 章 構成管理に関する要求

7.1 構成管理

対応する第 1 部の要求事項

会社は、6 章のサイバーリスクアセスメントの対象となる IT/OT 資産及びネットワーク構成について、現在の構成及び変更履歴を管理しなければならない。

評価基準

- ・ 6 章のサイバーリスクアセスメントの対象となる IT/OT 資産及びネットワーク構成について、現在の構成が文書化され、維持されていること。
- ・ 構成情報が更新された履歴（いつ、どの構成情報が更新されたか）が、台帳の一部として記録され、維持されていること。

求められる客観的証拠

構成情報を記録した文書（資産一覧、ネットワーク構成図等）が存在し、少なくとも以下が確認できること。

- ・ 6 章のリスクアセスメントの対象となる IT/OT 資産及びネットワーク構成の現在の状態が把握できること。
- ・ 資産一覧が船舶の運用期間を通じて維持・更新されていること（供給者等又は第三者による更新・保守を含む）。
- ・ 構成情報の更新履歴が台帳の一部として残されており、現在の構成がいつ時点のものが追跡できること。

外部要件の対応

- ・ IACS Rec. 194 : PROTECT, Item 9

7.2 変更管理

対応する第 1 部の要求事項

会社は、IT/OT 資産、ネットワーク構成、ソフトウェア又は外部接続の変更を管理する手順を定めなければならない。当該手順には、変更在先 6 章に定めるサイバーリスクアセスメントのプロセスに従いサイバーリスクを評価し、その結果に基づき 8 章に定める管理策の適用を見直した上で、変更を承認し、実施することを含めなければならない。

評価基準

- ・ IT/OT 資産、ネットワーク構成、ソフトウェア又は外部接続の変更を管理する手順が定められていること。
- ・ IT/OT 資産、ネットワーク構成、ソフトウェア又は外部接続に変更が生じる場合、変更前に 6 章に定めるサイバーリスクアセスメントのプロセスに従いサイバーリスクが評価され、その結果に基づき 8 章に定める管理策の適用が見直されていること。
- ・ 新たな技術又は機器を導入する場合、導入前にサイバーセキュリティの観点から評価する手順が定められていること。
- ・ 変更ごとに、その経緯（評価、承認、実施）が追跡できるよう記録されていること。

求められる客観的証拠

変更管理に関する手順が存在し、少なくとも以下が確認できること。

- ・変更管理の対象となる変更（IT／OT 資産，ネットワーク構成，ソフトウェア，外部接続の変更）が定められていること。
 - ・変更に関し 6 章に定めるプロセスに従いサイバーリスクを評価し，その結果に基づき 8 章に定める管理策の適用を見直すことが定められていること。
 - ・変更の承認者又は承認プロセスが定められていること。
 - ・新たな技術又は機器の導入に関しサイバーセキュリティ評価の手続が定められていること。
 - ・資格を有し，承認された要員が変更又は保守を実施することが定められていること。
- 変更の記録が存在する場合，少なくとも以下が確認できること。
- ・各変更について，変更前のリスク評価，その判断，及び実施の経緯が追跡できること。
 - ・評価結果が，6 章のサイバーリスクアセスメント及び 8 章の管理策の見直しに反映されていること。

注：定期的なソフトウェア更新は 8.c.2 による。

外部要件の対応

- ・ DryBMS（No. 28）：Advanced
- ・ IACS Rec. 194：IDENTIFY，PROTECT，Item 1，Item 9

7.3 構成の見直し

対応する第 1 部の要求事項

会社は，構成及び設定が承認済みの状態を保っていることを定期的に確認しなければならない。

評価基準

- ・ 構成及び設定が承認済みの状態を保っていることが，定期的に確認されていること。

求められる客観的証拠

構成の定期確認に関する記録が存在し，少なくとも以下が確認できること。

- ・ 構成及び設定が承認済みの状態と一致しているかを確認する仕組みが定められていること。
- ・ 定期的な確認が実施され，承認済みの状態とのずれが識別された場合の対応が記録されていること。

外部要件の対応

- ・ IACS Rec. 194：PROTECT，Item 9

8 章 管理策

8.a アクセス及び利用の管理

8.a.1 識別及び認証管理

評価基準

- ・ 実行可能な範囲において、利用者個人に固有の認証情報が割り当てられていること。運用上の理由により共用又は汎用の認証情報を使用する場合は、当該認証情報が管理された状態に置かれていること（例：使用者の範囲の限定、管理責任者の指定、乗組員交代時のパスワード変更）。
- ・ すべての機器においてデフォルトパスワードが変更されていること。
- ・ パスワードポリシーが定義され、適用されていること。
- ・ 共通のユーザープロファイル及びパスワードは乗組員交代時に変更され、引き継がれていないこと。外部要求事項上求められる場合は、パスワードの定期変更が実施されていること。
- ・ パスワードが端末に掲示されている等、管理されない状態に置かれていないこと。
- ・ 退職又は役割変更した要員のアカウントが速やかに無効化されていること。

求められる客観的証拠

アクセス制御の方針及び手順書が存在し、認証管理に関して少なくとも次が確認できること。

- ・ 固有の認証情報の割当て、パスワードポリシー及びアカウント管理（退職・役割変更時の無効化を含む）の要件が定められていること。
- ・ 乗組員交代時における共通プロファイル及びパスワードの変更及び引継ぎ禁止が定められていること。外部要求事項上求められる場合は、パスワードの定期変更要件が定められていること。

認証管理によるアクセス制御の実施状況を示す記録が存在し、少なくとも次が確認できること。

- ・ ユーザーアカウント一覧に管理されていない共用・共有アカウントが存在しないこと。共用又は汎用の認証情報を使用する場合は、当該認証情報の管理方法が確認できること（使用者の範囲、管理責任者、交代時変更等）。
- ・ 退職又は役割変更した要員のアカウントが無効化されていることが確認できること。

注：ユーザーアカウント一覧は **8.a.2** と同一文書により確認する。本項の確認点は共用・共有アカウント及び退職者等アカウントの無効化。

外部要件の対応

- ・ DryBMS (No. 28) : Intermediate
- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : 13.1.3, 13.2.4, 13.4.5
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.1, 3.5.3.2
- ・ IACS Rec. 194 : PROTECT, Item 4, Item 6

8.a.2 認可及び特権管理

評価基準

- ・管理者権限が、指定された上級士官又は承認された要員のみに制限されていること。
- ・ユーザープロファイルにより、システムの使用が本来の用途に制限されていること。
- ・ユーザープロファイルが適切に管理され、不要なプロファイルが削除されていること。
- ・船内ネットワークにおけるユーザープロファイル及びパスワード管理の責任者が指定されていること。

求められる客観的証拠

手順書その他の CSMS 文書において、少なくとも認可及び特権管理に関して以下が確認できること：

- ・管理者権限の付与対象者が定められていること。
 - ・ユーザープロファイル及びパスワード管理の責任者の指定が文書化されていること。
- 認可及び特権管理の実施状況を示す記録が存在し、少なくとも以下が確認できること。
- ・管理者権限の保有者が定められた範囲に限定されていること。
 - ・不要なプロファイルが削除されていること。

注：ユーザーアカウント一覧は **8.a.1** と同一文書により確認する。本項の確認点は管理者権限保有者の限定及び不要プロファイルの削除。

外部要件の対応

- ・ DryBMS (No. 28) : Intermediate
- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 1, Stage 4, 13.1.3, 13.4.5
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.1, 3.5.3.2
- ・ IACS Rec. 194 : PROTECT, Item 4

8.a.3 リモートアクセス及び第三者アクセスの管理

評価基準

- ・第三者（検査員・技術者等の訪問者を含む。アクセスの経路を問わない。）による IT 及び OT システムへのアクセスを規定する手順が存在し、機微な機器へのアクセスに正式な承認が要求されていること。
- ・リモートアクセス（船外からのアクセスをいい、会社の陸上要員によるものを含む。）について、船上責任者による明示的な承認、陸上側の承認された要員による管理、強力な認証（当該リモートアクセスの方式が対応している場合、多要素認証を含む）及び暗号化の使用が定められていること。
- ・外部要求事項上求められるリモートアクセスに関する措置が講じられていること（例：ログイン失敗回数の制限、船上要員による手動終了又は無操作時の自動終了、リモートセッションの活動ログの取得）。
- ・機微な IT/OT システムへの第三者アクセス及びリモートアクセスの承認記録が維持されていること。

求められる客観的証拠

第三者アクセス及びリモートアクセスに関する手順が存在し、少なくとも以下が確認できること：

- ・機微な IT/OT システムへのアクセス（ローカル及びリモート）の承認プロセスが定義されていること。
 - ・リモートアクセスのセキュリティ要件（多要素認証を含む認証、暗号化、ログイン失敗回数の制限、セッション終了、セッションログ）が記載されていること。
- アクセスの実施記録が存在し、少なくとも以下が確認できること：
- ・第三者アクセスの正式な承認記録が存在すること（アクセス者の身元、承認者、日時が記録されていること）。
 - ・リモートアクセスが利用された場合、セッションログが存在すること。

注：リモートセッションの活動ログは **8.e.1** と同一記録により確認する。本項の確認点は承認記録との対応。

外部要件の対応

- ・ DryBMS (No. 28) : Intermediate, Advanced
- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 1, Stage 2, Stage 4, 13.1.3, 13.2.4, 13.4.5
- ・ IACS Rec. 194 : PROTECT, Item 6

8.a.4 適切な利用及び利用者起因リスクの管理

評価基準

- ・ 正規の利用者（乗組員及び陸上要員）が IT 及び OT システムを利用する際に遵守すべき事項（許容される利用の範囲及び禁止行為。例：離席時の端末ロック、無許可ソフトウェアの不使用、ソーシャルメディアの責任ある使用）が定められ、周知されていること。
- ・ 船内での個人所有デバイスの使用に関する手順が定められていること。
- ・ 乗組員によるネットワークの利用が、認められた範囲に管理されていること。

求められる客観的証拠

- ・ 正規の利用者の遵守事項、個人所有デバイスの使用及び乗組員のネットワーク利用に関する規則が、手順書その他の CSMS 文書に定められていること。
- ・ 当該規則が要員に周知されていることを示す記録が存在すること（教育記録、配付記録等）。

注：8.a.4 の適合確認は、8.a.3, 8.b.1, 8.c.5 及び 8.d.1 を含む関連ドメインのエビデンスを横断的に判断することにより行う。

外部要件の対応

- ・ DryBMS (No. 28) : Intermediate
- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 1, Stage 2, Stage 4, 13.1.3, 13.2.4, 13.4.5
- ・ IACS Rec. 194 : PROTECT, Item 4, Item 5

8.b ネットワーク及び通信の保護

8.b.1 ネットワーク分離及びゾーニング

評価基準

- ・ 船内 IT 及び OT システムが、機能及びリスクに基づき、論理的又は物理的に分離されたネットワークゾーンとして構成されており、少なくとも次の分離が実施されていること。
- (1) OT ネットワークと IT ネットワークの分離（両者間の通信がファイアウォールその他のセキュリティ機器を経由して制御されていること）
- (2) 乗組員の個人利用ネットワーク（Crew ゾーン）の、業務用 IT 及び OT ネットワークからの分離
 - ・ 外部接続（衛星通信、リモートアクセス等）が、DMZ 又は同等のセキュリティゾーンを経由して管理され、業務用及び OT ネットワークへ直接接続されていないこと。
 - ・ ネットワークゾーンの構成及びゾーン間通信の制御ルールが文書化され、承認された状態が維持されていること。
 - ・ ゾーン設計が、6 章のサイバーリスクアセスメントの結果を踏まえて決定されていること。

求められる客観的証拠

船内 IT/OT ネットワーク構成図が存在し、少なくとも以下が確認できること。

- ・ ネットワークゾーンの区分及び名称が定義されていること（例：OT/Navigation, OT/Machinery, IT/Business, Crew, DMZ 等）。
 - ・ ゾーン間の接続関係及び外部接続点を示されていること。
 - ・ ゾーン間に設置されたセキュリティ機器の種別及び設置箇所が特定されていること。
- ゾーン間通信制御ルールを示す文書（ファイアウォールポリシー、ACL 等）が存在し、承認されたゾーン間通信ルールが定義されていること。
- サイバーリスクアセスメントの記録により、少なくとも以下が確認できること。
- ・ ネットワーク構成及びゾーン設計がリスクアセスメントの対象として取り扱われていること。
 - ・ ゾーン設計の判断根拠がリスクアセスメントの結果と関連付けられていること。

注：ネットワーク構成図は 6.4 及び 8.b.3 と同一文書により確認する。本項の確認点はゾーン設計及びゾーン間通信制御。

外部要件の対応

- ・ TMSA 3（Element 13）：Stage 4, 13.4.5
- ・ MSC-FAL.1/Circ.3/Rev.3：3.5.3.2, 3.5.3.3
- ・ IACS Rec. 194：PROTECT, Item 2, Item 5

8.b.2 通信の保護

評価基準

- ・ 使用する通信プロトコル及びサービスが特定され、管理されていること。
- ・ 不要又は未使用の通信サービス及びポートが無効化されていること。
- ・ 機微なデータの伝送において、適切な暗号化通信が使用されていること。

求められる客観的証拠

通信の管理に関する文書又は設定記録が存在し、少なくとも以下が確認できること。

- ・ 使用を許可する通信プロトコル及びサービスが特定されていること。
- ・ 不要又は未使用の通信サービス及びポートの無効化が、設定記録又は点検記録により確認できること。
- ・ 機微なデータの伝送に係る暗号化の要件が定められていること。

注：設定記録は **8.c.1** と同一記録により確認する。本項の確認点は通信サービス及びポートの無効化並びに暗号化要件。

外部要件の対応

- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・ IACS Rec. 194 : PROTECT, Item 2, Item 5, Item 6

8.b.3 外部接続の管理

評価基準

- ・ 外部接続（船外のネットワーク又はシステムとの接続経路をいい、衛星通信、遠隔保守、陸上－船舶インターフェース等を含む。接続する主体及びリモートアクセスに使用されるか否かを問わない。）が特定され、文書化され、管理されていること。
- ・ 新たな外部接続の確立に係る承認プロセスが定められていること。

求められる客観的証拠

外部接続の一覧又はネットワーク構成図が存在し、すべての外部接続点が特定され、文書化されていること。

新たな外部接続の承認に関する手順が存在し、承認記録が存在する場合には、承認者及び承認日が確認できること。

注：外部接続の一覧又はネットワーク構成図は **8.b.1** 及び **6.4** と同一文書により確認する。本項の確認点は外部接続点の網羅性及び新規接続の承認手順。

外部要件の対応

- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5

8.c システム構成及び保守

8.c.1 安全な構成及びハードニング

評価基準

- ・船内で使用するシステムについて、ベンダーのデフォルト構成をレビューし、不要なサービス、プロトコル及びアカウントの無効化その他必要なハードニングを実施するプロセスが定められていること（OT システムについては、供給者が許可する範囲で実施することが定められていること）。
- ・当該プロセスに基づき、レビュー及びハードニングが実施されていること。

求められる客観的証拠

構成基準又は設定記録が存在し、少なくとも以下が確認できること：

- ・不要なサービス、プロトコル及びアカウントの無効化に関する要件が定められ、又はその実施状況が記録により確認できること。
- ・デフォルト構成のレビュー及びハードニングの実施状況が記録により確認できること。

注：設定記録は 8.b.2 と同一記録により確認する。本項の確認点は不要なサービス・プロトコル・アカウントの無効化及びハードニングの実施。

外部要件の対応

- ・ DryBMS（No. 28）：Intermediate
- ・ TMSA 3（Element 13）：Stage 4, 13.4.5

8.c.2 パッチ及び更新管理

評価基準

・船内 IT 及び OT システムのソフトウェア及びファームウェアの更新を管理するプロセスが存在し、少なくとも次が定められていること。

(1) 更新の適用の頻度又はスケジュール（供給者の推奨又は供給者との合意に従う場合を含む）

(2) 更新を実施する者（資格を有し、承認された要員によることを含む）

(3) OT システムに係る供給者の関与又は許可の考慮

- ・更新及びパッチが、定められたプロセスに従い適用されていること。
- ・パッチ及び更新状況の記録が維持されていること。

求められる客観的証拠

パッチ及び更新管理の手順書が存在し、少なくとも以下が確認できること。

- ・評価基準（1）～（3）に掲げる事項が定められていること。

実施状況を示す記録が存在し、少なくとも以下が確認できること。

- ・船内システムの更新及びパッチ適用状況の記録が維持されていること。
- ・延期又は未実施の更新について、根拠が文書化されていること。

注：パッチ適用状況は 6.4 の資産一覧（パッチ更新状況）と同一情報源により確認できる場合がある。本項の確認点は適用プロセス・スケジュール及び未実施更新の根拠。

注：定められたプロセス又はスケジュールに従う定常的な更新は本項による。定常の範

囲を超える変更（システムの機能又は構成に影響を及ぼすバージョンアップ等）は、7.2に定める変更管理による。

外部要件の対応

- ・ DryBMS（No. 28）：Intermediate
- ・ SIRE 2.0：Section 7.5
- ・ TMSA 3（Element 13）：Stage 4, 13.4.5
- ・ MSC-FAL.1/Circ.3/Rev.3：3.5.3.3, 3.5.3.7
- ・ IACS Rec. 194：PROTECT, Item 9

8.c.3 陳腐化管理

評価基準

- ・ 製造者によるサポートが終了した、又は終了時期が判明しているシステム及びソフトウェアを特定するプロセスが定められていること。
- ・ 特定されたサポート終了システムに関連するリスクが、6章のサイバーリスクアセスメントにおいて考慮され、必要な管理策（例：補完的管理策）が決定され、実施されていること。

求められる客観的証拠

サポート終了システムの特定期に関する規定（手順書又は資産一覧の運用規定等）が存在し、少なくとも以下が確認できること。

- ・ サポート状況を特定・記録する方法が定められていること。

サポート終了システムに関する記録が存在し、少なくとも以下が確認できること。

- ・ サポート終了又はEOLのシステム及びソフトウェアが特定されていること。
- ・ 関連するリスク及び決定された管理策（補完的管理策を含む。例：ネットワーク分離の強化、外部接続・リモートアクセス及び物理ポートの制限、監視の強化、更改計画の策定等）が文書化されていること。

注：サポート状況は6.4の資産一覧（ソフトウェアバージョン、パッチ更新状況）と同一情報源により確認できる場合がある。リスクの評価自体は6.4による。本項の確認点はサポート終了システムの特定期及び管理策の実施。

外部要件の対応

- ・ DryBMS（No. 28）：Intermediate
- ・ TMSA 3（Element 13）：Stage 4, 13.4.5

8.c.4 マルウェア及びエンドポイント保護

評価基準

- ・ 船内コンピュータに対するマルウェア保護に関する規定が存在し、少なくとも次が定められていること。

- (1) 技術的に実現可能であり、かつ供給者による制限がない場合、ウイルス対策又は同等のマルウェア保護を適用すること
- (2) OT システムについては、システム供給者が許可又は提供している場合に限り適用すること
- (3) マルウェア保護の定義ファイル等を最新の状態に維持すること

- ・上記(1)～(3)を含む規定に従い、ECDIS を含む適用可能な船内コンピュータにマルウェア保護が適用され、最新の状態に維持されていること。

求められる客観的証拠

マルウェア保護に関する規定(手順書等)が存在し、少なくとも以下が確認できること。

- ・評価基準(1)～(3)の事項が定められていること。

実施状況を示す記録が存在し、少なくとも以下が確認できること。

- ・ECDIS を含む適用可能な船内コンピュータに、ウイルス対策又は同等のマルウェア保護が適用されていること。
- ・OT システムについて、供給者の許可又は提供の状況が文書化されていること。
- ・定義ファイル等の更新記録により、最新状態が維持されていることが確認できること。

外部要件の対応

- ・RISQ v3.2 : 12.8
- ・DryBMS (No. 28) : Intermediate
- ・SIRE 2.0 : Section 7.5
- ・TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.4
- ・IACS Rec. 194 : PROTECT, Item 3

8.c.5 ハードウェアおよびソフトウェアの管理

評価基準

- ・船内での使用に先立ち、ハードウェア及びソフトウェアを承認するプロセスが確立されており、当該プロセスにおいて、機器及びシステムの設計上のサイバーレジリエンス(例：IACS UR E27 等の国際的な基準への適合や型式承認の有無、会社が定める搭載条件への適合等)が考慮事項とされていること。
- ・未承認のソフトウェアが船内システムにインストールされていないこと。
- ・データ消去を含む機器の安全な廃棄に関する手順が存在すること。

求められる客観的証拠

ハードウェア及びソフトウェア管理の手順書が存在し、少なくとも以下が確認できること。

- ・船内での使用前の承認プロセスが定義されていること。
- ・承認における考慮事項として、機器又はシステムのサイバーセキュリティに関する適合状況等(例：IACS UR E27 等の国際的な基準への適合や型式承認の有無、会社が定める搭載条件への適合)が含まれていること。
- ・データ消去を含む機器の安全な廃棄が手順に含まれていること。

実施状況を示す記録が存在し、少なくとも以下が確認できること。

- ・ハードウェア及びソフトウェアの承認記録が存在すること。
- ・船内システムにインストールされているソフトウェアが把握され、未承認のソフトウェアが存在しないことが確認されていること。

注：使用前の承認プロセスは、7.2 の変更管理手順と同一文書により確認できる場合がある。本項の確認点はモノ(ハードウェア及びソフトウェア)の承認及び廃棄。

外部要件の対応

- DryBMS (No. 28) : Intermediate
- SIRE 2.0 : Section 7.5
- TMSA 3 (Element 13) : Stage 2, Stage 4, 13.2.4, 13.4.5
- MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.3, 3.8

8.d 媒体及び物理インターフェース管理

8.d.1 可搬媒体の管理

評価基準

- ・管理されたシステムへのデータ転送に可搬媒体（USB メモリ，CD/DVD，外付け HDD 等）を通常使用しないことが，方針として文書化されていること。
- ・やむを得ず可搬媒体を使用する場合の例外管理プロセス（許可条件及び承認要件）が定められていること。
- ・可搬媒体の使用前に，最新の状態に維持されたマルウェア対策によるスキャンを実施することが要求されていること。外部要求事項上求められる場合は，当該要求に応じた方法によること（例：船舶の制御ネットワークに接続されていないコンピュータでのスキャンの実施）。

求められる客観的証拠

可搬媒体管理の方針・手順書が存在し，少なくとも以下が確認できること。

- ・管理されたシステムへの可搬媒体使用の原則禁止が明記されていること。
- ・例外使用の条件及び承認プロセスが定義されていること。
- ・使用前のマルウェアスキャン要件が定められていること。

実施状況を示す記録が存在し，少なくとも以下が確認できること。

- ・例外使用の承認記録が存在すること（承認者及び承認日が記録されていること）。
- ・マルウェアスキャンの実施が記録により確認できること（外部要求事項上求められる場合は，船舶の制御ネットワークに接続されていないコンピュータでの実施を含む）。
- ・方針及び手順が陸上・船上の要員に周知されていることを示す記録が存在すること（教育記録，配付記録等）。

外部要件の対応

- ・RISQ v3.2 : 12.8
- ・DryBMS (No. 28) : Intermediate
- ・SIRE 2.0 : Section 7.5
- ・TMSA 3 (Element 13) : Stage 1, Stage 2, Stage 4, 13.1.3, 13.2.4, 13.4.5
- ・MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.5
- ・IACS Rec. 194 : PROTECT, Item 7

8.d.2 物理ポート及びインターフェースの保護

評価基準

- ・未使用の物理ポート（USB，RJ-45 等）が，物理プラグ又は同等の措置により，恒常的かつ一貫してブロックされていること。
- ・鍵又はブロック器具が，承認された要員のみによって管理されていること。
- ・資産一覧において特定された，物理的にアクセス可能なすべてのコンピュータ及びネットワークポートが保護措置の対象となっていること。
- ・ECDIS 等の重要システムの USB 及び RJ-45 ポートへのアクセスが，ポートの無効化又は施錠により制御されていること。

求められる客観的証拠

保護対象機器・ポート一覧が存在し，少なくとも以下が確認できること。

- ・対象機器名及びポート種別（USB、RJ-45 等）が特定されていること。
- ・ECDIS 等の重要システムが対象として含まれ、USB 及び RJ-45 ポートが取り扱われていること。
- ・各ポートに適用されている保護措置の種別が記載されていること。

物理的保護措置の実施確認記録（点検記録、写真等）が存在し、少なくとも以下が確認できること。

- ・ポートブロッカー等の設置状況が記録又は写真等で確認できること。
- ・鍵又は器具の管理者が特定されていること。

注：保護対象機器・ポート一覧は、7.1 の資産一覧を基礎として作成されている場合、同一文書により確認できる。本項の確認点は保護措置の種別及び実施状況。

外部要件の対応

- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・ IACS Rec. 194 : PROTECT, Item 7

8.d.3 直接接続の管理

評価基準

- ・ 船内システムへの直接接続（作業用 PC，保守端末，外部機器等によるもの）を規定する手順が存在し，承認なしの直接接続が禁止されていること。
- ・ 承認プロセス，接続条件及び接続中の監視要件が定義されていること。
- ・ 供給者・保守要員等の第三者による直接接続の管理要件が定義され，接続の記録が維持されていること。

求められる客観的証拠

直接接続管理の手順書が存在し，少なくとも以下が確認できること。

- ・ 承認なしの直接接続の禁止が明記されていること。
- ・ 承認プロセス，接続条件及び第三者への管理要件が定義されていること。

直接接続の承認記録が存在し，少なくとも以下が確認できること。

- ・ 接続の目的，接続者，承認者及び接続日時が記録されていること。

注：第三者による直接接続の承認は，8.a.3 の第三者アクセスの承認と同一の記録により確認できる場合がある。本項の確認点は，接続の条件（持込機器の事前確認を含む）及び接続中の管理並びに接続の記録。

注：接続中の人的な立会い・帯同について，ISPS コードに基づく船舶保安計画（SSP）の訪問者管理の規定によることとしている場合は，CSMS 文書において当該規定が参照されていることを確認すれば足りる。持込機器の接続条件の確認は本項による。

外部要件の対応

- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5

8.d.4 物理アクセスの管理

評価基準

- ・ 機微な IT/OT 機器が設置されている区画（機関室，ブリッジ，サーバー室等）が施錠

され、権限のない者によるアクセスが防止されていること。区画単位で管理できないネットワーク機器等については、設置場所又は筐体の施錠その他の措置により保護されていること。

- ・当該区画へのアクセス権限を有する者が定義され、文書化されていること。
- ・権限のない者による立入り又はその形跡を認めた場合に報告することが定められていること（報告後の対応は **9.1** による）。

求められる客観的証拠

物理アクセス管理の手順書が存在し、少なくとも以下が確認できること。

- ・ 管理対象区画及び区画外で保護すべき機器が特定されていること。
- ・ アクセス権限を有する者が定義されていること。
- ・ 権限のない立入りを認めた場合の報告について定められていること。

アクセス権限者リストが存在し、少なくとも以下が確認できること。

- ・ 管理対象区画ごとにアクセス権限者が特定され、当該リストが最新状態に維持されていること。

注：区画への立入り管理について、ISPS コードに基づく船舶保安計画（SSP）の関連規定によることとしている場合は、CSMS 文書において当該規定が参照されていることを確認すれば足りる。なお SSP の内容の適否は本審査の対象としない。

外部要件の対応

- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・ IACS Rec. 194 : PROTECT, Item 4

8.e 監視, ログ及び検知

8.e.1 イベントログ管理

評価基準

- ・船内 IT 及び OT システムにおいてセキュリティ関連イベントをログに記録することが定められていること。記録の対象には、技術的に実現可能な範囲において、少なくとも次を含むこと。

- (1) 認証イベント
- (2) 管理者権限の使用
- (3) 構成変更
- (4) リモートセッション活動
- (5) ネットワーク境界又は外部接続点における通信

- ・ログの取得が、ネットワークセキュリティ機器を含む該当する機器又はシステムにおいて有効化されていること。
- ・取得したログが、侵入検知及びインシデント対応に利用できるよう、収集され、参照可能な状態で保持されていること（保存時の保護は **8.e.3** による）。

注：ログの一元的な収集（陸上への転送を含む）は、インシデント発生時の調査及びログレビューの実行力を高めるため、通信環境等の制約の範囲で採用することが望ましい。

求められる客観的証拠

ログの取得に関する規定（手順書等）が存在し、少なくとも以下が確認できること。

- ・取得するログの種別及び取得対象のシステム・機器が定められており、技術的に実現可能な範囲において評価基準**(1)～(5)**が含まれていること。
- ・ログの収集及び保管の方法が、ログの保管容量の制約（ローカル保存における上書き等）を考慮した上で定められていること。

ログが取得されていることを示す証拠（設定記録、ログの現物等）が存在し、少なくとも以下が確認できること。

- ・ネットワークセキュリティ機器（IT/OT 境界のファイアウォール等）においてログが設定されていること。
- ・規定に従いログが収集され、保管されていること。

注：ネットワークセキュリティ機器の設定記録は **8.e.2** と同一文書により確認する。本項の確認点はログ種別及び保管。リモートセッションの活動ログは **8.a.3** と共通。

外部要件の対応

- ・DryBMS（No. 28）：Excellence
- ・TMSA 3（Element 13）：Stage 4, 13.4.5
- ・MSC-FAL.1/Circ.3/Rev.3：3.5.3.3, 3.4, 3.4.1
- ・IACS Rec. 194：PROTECT, DETECT, Item 6, Item 10

8.e.2 セキュリティ監視

評価基準

- ・ネットワーク境界及び外部接続点において、技術的に実現可能な範囲で、ネットワークトラフィックの監視及びログの記録が可能となっていること。

- ・ IT/OT 境界においては、ファイアウォール又は同等のネットワークセキュリティ機器が、ネットワークトラフィックの監視、異常の検知、リアルタイムアラート及びログの記録の機能を有していること。
- ・ 当該境界及び外部接続点におけるトラフィックが監視されていること。
- ・ 検知された異常が通知される先（船上又は陸上の担当）が定められていること。

求められる客観的証拠

ネットワークセキュリティ機器（例：ファイアウォール、UTM、ファイアウォール機能を有する通信ゲートウェイ等）の機能を示す文書（仕様書、設定記録等）が存在し、少なくとも以下が確認できること。

- ・ 当該機器が、ネットワークトラフィックの監視、異常の検知、リアルタイムアラート機能及びログ生成を提供していること。
- ・ IT/OT 境界のトラフィックが監視対象となっていること。

監視の運用を示す規定又は記録が存在し、少なくとも以下が確認できること。

- ・ 検知された異常の通知先（船上又は陸上の担当。外部の監視サービスを利用する場合はその窓口）が定められていること。

注：ネットワークセキュリティ機器の仕様書・設定記録は **8.e.1** と同一文書により確認する。本項の確認点は監視・アラート機能及びその通知先。

外部要件の対応

- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.3, 3.4, 3.4.1
- ・ IACS Rec. 194 : PROTECT, DETECT, Item 2, Item 10

8.e.3 ログの保全及び保存

評価基準

- ・ ログが、不正な変更、削除又は上書きから保護された方法で保存されていること。
- ・ 保存されたログへのアクセス権限が、**8.a.2** に従い管理されていること。
- ・ ログの最低保存期間が定義され、実施されていること。

求められる客観的証拠

ログの保存に関する規定（手順書等）が存在し、少なくとも以下が確認できること。

- ・ ログの最低保存期間が定められていること。
- ・ ログを不正な変更、削除又は上書きから保護する方法（例：ログが保存された機器・媒体への物理アクセスの制限、陸上への転送等）が定められていること。
- ・ 保存されたログへのアクセス権限の管理が定められていること（管理の内容は **8.a.2** による）。

ログの保存状況を示す証拠が存在し、少なくとも以下が確認できること。

- ・ 規定に従いログが保存されていること（例：保存されたログの範囲・期間の確認）。

外部要件の対応

- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.3
- ・ IACS Rec. 194 : DETECT, Item 10

8.e.4 ログのレビュー及び異常調査

評価基準

- ・保存されたログを，会社が定める頻度又は契機によりレビューするプロセス（外部によるレビューを含む）が定められていること。
- ・検知され又は報告された異常若しくは不審なイベントを調査し，必要に応じてエスカレーションするプロセスが定められていること。当該調査において，保存されたログを利用することが定められていること。
- ・ログのレビュー，調査及びエスカレーションに関する責任が定義されていること。

求められる客観的証拠

ログのレビュー並びに異常の調査及びエスカレーションに関する手順書が存在し，少なくとも以下が確認できること。

- ・ログレビューの頻度又は契機が定められていること。
- ・ログレビュー及び調査の責任者又は担当が定義されていること（外部サービスに委託する場合はその窓口を含む）。
- ・調査において保存されたログを利用することが定められていること。
- ・エスカレーションの経路が定義されていること。

注：異常の検知及び通知先は 8.e.2，報告された事象の評価及びインシデントとしての対応は 9.1 による。本項の確認点は，ログのレビュー並びに検知又は報告から調査・エスカレーションに至る流れ。本項の手順は，9.1 のサイバーインシデント対応手順と同一文書により確認できる場合がある。

外部要件の対応

- ・ TMSA 3 (Element 13) : Stage 4, 13.4.5

8.f バックアップ及び復旧

8.f.1 バックアップ方針及び実施

評価基準

- ・航行、推進及び運航に重要な船内デジタルシステムについて、バックアップ方針が存在すること。
- ・バックアップが定義されたスケジュールで実施され、復旧を可能にする方法で保持されていること。
- ・バックアップ機能が整備されており、サイバーインシデント発生後の復旧支援に利用できる状態にあること。
- ・OT システムについて、旗国の法定規則又は船級規則が要求するシステム・機器の二重化、又は供給者が提供し若しくは会社が策定したバックアップ・復旧手順の少なくとも一方が整備されていること。

求められる客観的証拠

バックアップ方針（手順書等）が存在し、少なくとも以下が定められていることが確認できること。

- ・何を：バックアップの対象とするシステム（航行、推進及び運航に重要なシステムのうち、6 章のリスクアセスメントを踏まえて会社が定めるもの）
- ・いつ：バックアップの頻度又は契機（例：定期、海図・設定の更新後、航海毎等）
- ・どう保持するか：保存先及び保持の方法（例：外部媒体への保存と船内保管、陸上への複製の送付等）
- ・OT システムの扱い：二重化によるか、バックアップ・復旧手順によるか（又はその両方か）

バックアップの実施状況を示す記録が存在し、少なくとも以下が確認できること。

- ・既定のスケジュールに従いバックアップが実施されていること（例：バックアップログ、直近の実施記録）。
- ・OT システムについて、二重化の根拠（法定規則・船級規則の該当）又は供給者若しくは会社のバックアップ・復旧手順の存在が確認できること。

注：二重化による場合、当該法定規則又は船級規則への適合自体は本審査の対象としない。CSMS 文書において当該規則が根拠として参照されていることを確認すれば足りる。

注：安全要件としての二重化は、機器の故障に対する冗長性を目的とするものであり、サイバーインシデントに対する復旧能力を当然には保証しない（例：法定要件により 2 台搭載される ECDIS が、同一のネットワーク又は更新経路を共有している場合、マルウェア感染が両方に及び得る）。会社は、外部との接点を有するシステムについて、6 章のサイバーリスクアセスメントにおいてこの点を考慮することが望ましい。

外部要件の対応

- ・SIRE 2.0 : Section 7.5
- ・TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・MSC-FAL.1/Circ.3/Rev.3 : 3.5.1
- ・IACS Rec. 194 : RECOVER, Item 13

8.f.2 復旧手順

評価基準

- ・サイバーインシデント発生後に、**8.f.1** に規定するバックアップ方針の対象システムを復旧するための手順が文書化されており、システムごとに、適切な復旧手段（例：バックアップからの復元、二重化系への切替え、予備機への交換、供給者による復旧）及び実施者又は依頼先が定められていること。このうち航行及び推進に重要な OT システムについては、迅速かつ安全な復旧の観点から具体的に定められていること。
- ・複数の対象システムに影響が及んだ場合の復旧の優先順位又は順序の考え方が定められていること。
- ・復旧したシステムについて、正常な状態であることを確認した上で運用に復帰することが定められていること。二重化系又は予備機による切替を行った場合に、元の構成に復帰するまでの考え方が定められていること。

注：サイバーインシデントへの対応の全体は **9 章** による（対応体制・報告は **9.1**，操練は **9.2**，支援の確保は **9.3**）。**8.f.2** 及び **8.f.3** の確認点は、システムを復旧する技術的手順（復旧の優先順位の考え方を含む）及びその検証であり，検証には **9.2** の操練を活用できる。本項の手順は，**9.1** のサイバーインシデント対応手順と同一文書により確認できる場合がある。

求められる客観的証拠

復旧手順の文書が存在し，少なくとも以下が確認できること。

- ・**8.f.1** に定めるバックアップ方針の対象システムが復旧の対象とされていること。
- ・システムごとに，適切な復旧手段（例：バックアップからの復元，二重化系への切替え，予備機への交換，供給者による復旧）及び実施者又は依頼先（供給者の連絡先を含む）が定められていること。
- ・航行及び推進に重要な OT システムが，迅速かつ安全な復旧の観点から具体的に取り扱われていること。
- ・複数の対象システムに影響が及んだ場合の復旧の優先順位又は順序の考え方が定められていること。
- ・復旧後の正常性確認が定められていること。
- ・二重化系又は予備機による運用からの復帰の考え方が定められていること。

外部要件の対応

- ・SIRE 2.0 : Section 7.5
- ・TMSA 3 (Element 13) : Stage 4, 13.4.5
- ・MSC-FAL.1/Circ.3/Rev.3 : 3.5.1, 3.5.3.7
- ・IACS Rec. 194 : RECOVER, Item 13

8.f.3 バックアップ及び復旧手順の検証

評価基準

- ・会社が取得し保持するバックアップについて，復元できることが，リストアテスト又は同等の検証（例：試験的な復元，媒体・ファイルの読取り確認）により定期的に確認されていること。
- ・**8.f.2** に定める復旧の体制について，次の確認が行われていること。

- (1) 体制の内容が最新であることの定期的な確認（例：供給者の連絡先の有効性，二重化の構成に変更がないこと）
- (2) 機能することの確認（例：二重化系への切替えの確認（法定・船級検査における確認を含む），操練（9.2）における復旧手順の使用）

注：サイバーインシデントへの対応の全体は9章による（対応体制・報告は9.1，操練は9.2，支援の確保は9.3）。8.f.2 及び 8.f.3 の確認点は，システムを復旧する技術的手順（復旧の優先順位の考え方を含む）及びその検証であり，検証には9.2 の操練を活用できる。本項の手順は，9.1 のサイバーインシデント対応手順と同一文書により確認できる場合がある。

求められる客観的証拠

バックアップの検証に関する記録が存在し，少なくとも以下が確認できること。

- ・ 検証の頻度又は契機が定められていること。
- ・ リストアテスト又は同等の検証が実施され，結果が記録されていること。

復旧体制の確認に関する記録が存在し，少なくとも以下が確認できること。

- ・ 体制の内容が最新であることの確認（供給者の連絡先，二重化の構成等）が定期的実施され，記録されていること。
- ・ 機能することの確認が実施され，記録されていること（例：検査における切替え確認の記録，操練の記録）。

外部要件の対応

- ・ TMSA 3（Element 13）：Stage 4，13.4.5
- ・ MSC-FAL.1/Circ.3/Rev.3：3.5.1
- ・ IACS Rec. 194：RECOVER，Item 13

9 章 緊急事態対応に関する要求

9.1 緊急事態への対応手順の確立

対応する第 1 部の要求事項

会社は、遭遇する可能性のある船舶のサイバーインシデント及びそれに起因する緊急事態を識別し、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。

評価基準

- ・ 想定されるサイバーインシデント及びそれに起因する緊急事態が識別されていること。
 - ・ 識別された事態に対応するための手順が文書化されていること。
 - ・ 手順には少なくとも次が含まれていること。
- (1) サイバーインシデントの予兆となり得る事象を識別し、会社へ報告する仕組み。当該事象には、船内ではサイバーインシデントに該当するか判断できないデジタル機器又はネットワークの異常を含む。
 - (2) 報告された事象がサイバーインシデントに該当するかを評価する仕組み
 - (3) 船内における対応手順及び報告経路
 - (4) 船舶と陸上組織との連携及び陸上側連絡窓口
 - (5) 外部当局への報告
 - (6) サイバーインシデントの記録
 - ・ 手順が非電子形式でも利用可能であること。
 - ・ 外部要求事項上求められる事態への対応が手順に含まれていること(例：航法機器の可用性喪失、GNSS 等外部データソースの喪失、GMDSS 通信を含む陸上との接続性喪失、推進・操舵等重要システムの制御機能喪失、ランサムウェア・DoS 攻撃)。

求められる客観的証拠

- サイバーインシデント対応手順（計画）が存在し、少なくとも以下が確認できること。
- ・ 想定されるサイバーインシデント及びそれに起因する緊急事態が列挙されていること。
 - ・ 船内対応手順、報告経路（船内・船陸間・外部当局への報告）が定められていること。
 - ・ 陸上側連絡窓口が特定されていること。
 - ・ サイバーインシデントの記録に関する要件が定められていること。
 - ・ 外部要求事項上求められる事態（航法機器喪失、GNSS 喪失、GMDSS 喪失、推進・操舵喪失、ランサムウェア・DoS）が対応対象として含まれていること。
- 手順が非電子形式（紙媒体等）でも利用可能であることが確認できること。
- 技術サポートの連絡先（会社の IT 部門又は外部 IT 業者等）が容易に参照できる状態にあること。

外部要件の対応

- ・ DryBMS (No. 28) : Basic
- ・ SIRE 2.0 : Section 7.5
- ・ TMSA 3 (Element 13) : Stage 1, 13.1.3, 13.1.5
- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3, 3.5.3.7, 3.5.5, 3.5.5.1, 3.5.5.2, 3.5.6, 3.5.6.1
- ・ IACS Rec. 194 : RESPOND, RECOVER, Item 12, Item 14

9.2 緊急事態への対応プログラムの確立

対応する第1部の要求事項

会社は、サイバーインシデント及びそれに起因する緊急事態への対応に備えるため、操練のプログラムを確立しなければならない。

評価基準

- ・サイバーインシデント及びそれに起因する緊急事態への対応に備えるための操練のプログラムが確立されていること。
- ・プログラムに基づき操練が実施されていること。
- ・操練の実施後、結果がレビューされ、識別された改善点が記録されていること。

求められる客観的証拠

操練のプログラムを定めた文書が存在し、少なくとも以下が確認できること。

- ・実施頻度又はスケジュールが定められていること。

操練の実施記録が存在し、少なくとも以下が確認できること。

- ・プログラムに基づき実施されていること。
- ・実施日及び参加者が記録されていること。
- ・事後レビュー（デブリーフィング等）が実施され、識別された改善点及び合意された是正措置が記録されていること。

外部要件の対応

- ・TMSA 3 (Element 13) : Stage 1, 13.1.3
- ・MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.6, 3.4, 3.5.5

9.3 緊急事態への対応を確保する手段の提供

対応する第1部の要求事項

会社は、サイバーインシデントへの対応に必要な支援を平時から確保しなければならない。

評価基準

- ・サイバーインシデントへの対応に必要な支援が平時から確保されていること。
- ・少なくとも、船舶に搭載されたシステムの供給者のうちサイバーインシデントに対応し得る担当者又は窓口が識別されていること。
- ・必要に応じ、専門的サイバー支援（コンサルタント等）との契約又は提携が確保されていること。

求められる客観的証拠

サイバーインシデント対応に必要な支援体制を示す文書又は記録が存在し、少なくとも以下が確認できること。

- ・船舶に搭載されたシステムの供給者のうち、サイバーインシデントに対応し得る担当者又は窓口が識別され、記録されていること。
- ・必要に応じ、専門的サイバー支援との契約又は提携に関する記録が存在すること。

外部要件の対応

- ・SIRE 2.0 : Section 7.5
- ・IACS Rec. 194 : RESPOND, RECOVER, Item 11, Item 14

10 章 不適合及び是正措置に関する要求

10.1 不適合の報告及び分析

対応する第 1 部の要求事項

会社は、不適合が会社に報告され、CSMS の有効性の向上を目的として調査及び分析されることを確保する手順を確立しなければならない。

評価基準

- ・ 不適合が会社に報告されることを確保する手順が文書化されていること。
- ・ 不適合の報告先が明確に定められていること。
- ・ 報告された不適合について、根本原因分析を含む調査及び分析が、CSMS の有効性の向上を目的として実施される仕組みが定められていること。
- ・ 分析を実施する責任者及び時期が定められていること。

求められる客観的証拠

不適合の報告及び分析に関する手順が存在し、少なくとも以下が確認できること。

- ・ 不適合の報告先（報告を受ける役割又は部署）が明確に定められていること。
- ・ 報告の経路、方法及び様式が定められていること。
- ・ 報告された不適合について、根本原因分析を行うことが定められていること。
- ・ 分析を実施する責任者及び時期が定められていること。

不適合の処理記録が存在する場合、少なくとも以下が確認できること。

- ・ 報告された不適合について、根本原因分析が実施されていること。

外部要件の対応

—

10.2 是正措置及び再発防止策

対応する第 1 部の要求事項

会社は、再発防止策を含む是正措置を実施するための手順を確立しなければならない。

評価基準

- ・ 根本原因分析の結果に基づき、再発防止策を含む是正措置計画を策定し、実施するための手順が文書化されていること。
- ・ 是正措置計画の実施責任者、実施時期及び承認者が定められていること。

求められる客観的証拠

是正措置に関する手順が存在し、少なくとも以下が確認できること。

- ・ 根本原因分析の結果に基づき、再発防止策を含む是正措置計画を策定することが定められていること。
- ・ 是正措置計画について、実施責任者、実施時期及び承認者が明確に定められていること。

是正措置の記録が存在する場合、少なくとも以下が確認できること。

- ・ 是正措置計画が策定され、承認されていること。
- ・ 計画に従い是正措置が実施され、その結果が記録されていること。

11 章 文書管理に関する要求

11.1 文書管理手順の確立及び維持

対応する第 1 部の要求事項

- 1. 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。
- 2. 前-1.の文書管理手順においては、少なくとも下記が規定されていること。
 - (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確認されており、承認されていること、及び
 - (3) 廃止文書はすみやかに取り除かれていること。

評価基準

- 1. CSMS に関連するすべての文書及びデータを管理する手順が文書化され、維持されていること。
- 2. 前-1.の文書管理手順においては、少なくとも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、船舶において利用可能であること
 - (2) 文書の変更が、関係する責任者による審査及び承認を経て行われること
 - (3) 廃止文書が速やかに撤去され、又は誤って使用されないよう管理されていること
 - (4) CSMS に関連する文書及びデータが、不正なアクセス、削除又は改ざんから保護されていること

求められる客観的証拠

文書管理手順が存在し、少なくとも以下が確認できること。

- ・ CSMS に関連する文書及びデータの管理方法が定められていること。
- ・ 文書の版管理及び配付管理（関連部署での有効版の使用）が定められていること。
- ・ 文書の変更に係る審査及び承認の責任者並びにプロセスが定められていること。
- ・ 廃止文書の除去方法が定められていること。
- ・ 文書及びデータの保護方法（例：アクセス権限の設定、保管場所の管理）が定められていること。

外部要件の対応

- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.6

11.2 サイバーセキュリティマネジメントマニュアル

対応する第 1 部の要求事項

会社は、CSMS を記述する文書を「サイバーセキュリティマネジメントマニュアル」として作成し、会社の公式文書として維持しなければならない。当該マニュアルは、会社に適用される文書及び各対象船舶に適用される文書から構成される。文書化の様式は、会社が最も効果的と判断するものとするができる。会社は、各船舶に、本船に適用される文書を船内に備えなければならない。

評価基準

- ・ CSMS を記述する文書が「サイバーセキュリティマネジメントマニュアル」として作成され、会社の管理文書として維持されていること。

- ・当該マニュアルが、会社に応用される文書及び各対象船舶に適用される文書により構成されていること。
- ・本ガイドラインで要求される事項が、いずれかの文書に記載されているか識別されていること。
- ・各対象船舶に、本船に適用される文書が船内に備えられていること。

注：各対象船舶に適用されるマニュアルは、会社に応用されるマニュアルを基礎とし、これに当該船舶の固有情報を加えて作成されることが想定される。

求められる客観的証拠

サイバーセキュリティマネジメントマニュアル（名称は問わない。）が存在し、少なくとも以下が確認できること。

- ・CSMS を記述する文書が会社の管理文書として位置づけられていること（承認、管理文書としての発行等が確認できること）。
- ・本ガイドラインで要求される事項が、いずれの文書に記載されているか識別されていること（文書一覧、対応表等）。
- ・マニュアルが、会社に応用される文書及び各対象船舶に適用される文書により構成されていること。
- ・各対象船舶について、本船に適用される文書が船内に備えられていること。

外部要件の対応

—

12 章 会社による検証，見直し及び評価に関する要求

12.1 内部サイバーセキュリティ監査

対応する第 1 部の要求事項

- 1. 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，会社及び船舶に対し 12 か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。
- 2. 監査を行う者は，被監査部署から独立し，かつ，サイバーセキュリティに関する監査を適切に実施するために必要な力量を有していなければならない。
- 3. 会社は監査の結果を関係する部署の責任者に周知しなければならない。監査において摘出された不適合は，10 章に定める是正措置の手順に従い処理しなければならない。

評価基準

- 1. 内部サイバーセキュリティ監査の実施及び実施方法について，以下を満たすこと。
 - ・サイバーセキュリティに関する活動が CSMS に従って実施されているかを検証するため，会社及び船舶に対し，12 か月を超えない間隔で内部サイバーセキュリティ監査が実施されていること。
 - ・監査が，文書化された手順及び監査計画に基づき実施されていること。
- 2. 監査員の独立性及び力量について，以下を満たすこと。
 - ・監査を行う者が，被監査部署から独立していること。
 - ・監査を行う者が，サイバーセキュリティに関する監査を適切に実施するために必要な力量を有していること。
- 3. 監査結果及び不適合への対応について，以下を満たすこと。
 - ・監査の結果が，関係する部署の責任者に周知されていること。
 - ・監査において摘出された不適合が，10 章に定める是正措置の手順に従い処理されていること。

求められる客観的証拠

内部監査に関する手順及び監査計画が存在し，少なくとも以下が確認できること。

- ・監査の対象範囲，頻度（12 か月を超えない間隔），方法が定められていること。
- ・監査の対象範囲に，CSMS 文書（方針及び手順）への準拠に加え，その実施状況が含まれていること。
- ・監査員の独立性及び必要な力量に関する要件が定められていること。

内部サイバーセキュリティ監査の実施記録が存在し，少なくとも以下が確認できること。

- ・会社及び船舶に対し，12 か月を超えない間隔で監査が実施されていること。
- ・監査を行った者が，被監査部署から独立しており，サイバーセキュリティに関する監査を適切に実施するために必要な力量を有していること（力量の確認は 4 章の記録による）。
- ・監査結果が関係する部署の責任者に周知されていること。
- ・摘出された不適合について，10 章に定める是正措置の手順に従い処理されていること。

外部要件の対応

- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.9

12.2 サイバーセキュリティマネジメントシステムの評価

対応する第1部の要求事項

トップマネジメントは、CSMSの有効性を定期的に見直さなければならない。会社は、見直しの結果を関係する部署の責任者に周知しなければならない。

評価基準

- ・ トップマネジメントが、CSMSの有効性を会社が定めた周期で見直していること。
- ・ 見直しにおいて、CSMSの有効性（適切性、妥当性及び有効性）が評価されていること。
- ・ 見直しにおいて、少なくとも以下がレビューされていること。
- ・ 内部監査の結果
- ・ サイバーリスクアセスメントの状況
- ・ サイバーインシデント及び不適合の状況
- ・ 是正措置の状況
- ・ 見直しの結果が、関係する部署の責任者に周知されていること。

求められる客観的証拠

マネジメントレビューの実施記録が存在し、少なくとも以下が確認できること。

- ・ トップマネジメントにより、CSMSの有効性を見直しが、会社が定めた周期で実施されていること（例：マネジメントレビュー議事録）。
- ・ 見直しにおいて、少なくとも内部監査の結果、サイバーリスクアセスメントの状況、サイバーインシデント及び不適合の状況、是正措置の状況がレビューされていること。
- ・ 見直しにおいて、CSMSの有効性（適切性、妥当性及び有効性）が評価されていること。
- ・ 見直しの結果が、関係する部署の責任者に周知されていること。

外部要件の対応

- ・ MSC-FAL.1/Circ.3/Rev.3 : 3.5.3.9, 3.6

一般財団法人 日本海事協会

船舶管理システム部

〒102-0094 東京都千代田区紀尾井町3番3号

Tel: 03-5226-2173

Email: met@classnk.or.jp

www.classnk.or.jp