1. 組織規程

SMS 文書番号 No.： **章番号：**
作成者：管理責任者 **承認者：**
件名：組織規程(抜粋)

1. 目的

この規則は、SMSを実施する部署および担当者の責任と権限の範囲を定義するものである。また、会社の経営活動が、安全運航ならびに環境保全の規則に確実に準拠するために、部署と担当者の相互関係を明確にしている。

(省略)

4.5　IT管理責任者
4.5.1 IT管理責任者の任務は以下の通りである。
(1)　船陸ともに、本船ITシステムの適切な操作を確実にすること。
(2)　IT関連のインシデント対応を監視、評価、補佐すること。
(3)　ITシステムに関連した必要な訓練と教育を行う。
(4)　ITシステムに関わるデータを管理する。
(5)　IT分野におけるサイバーリスクを把握しておくこと。
4.5.2　外部のITシステムのコンサルタントや専門家に、必要に応じ、ITについて相談できるように契約を締結することがある。

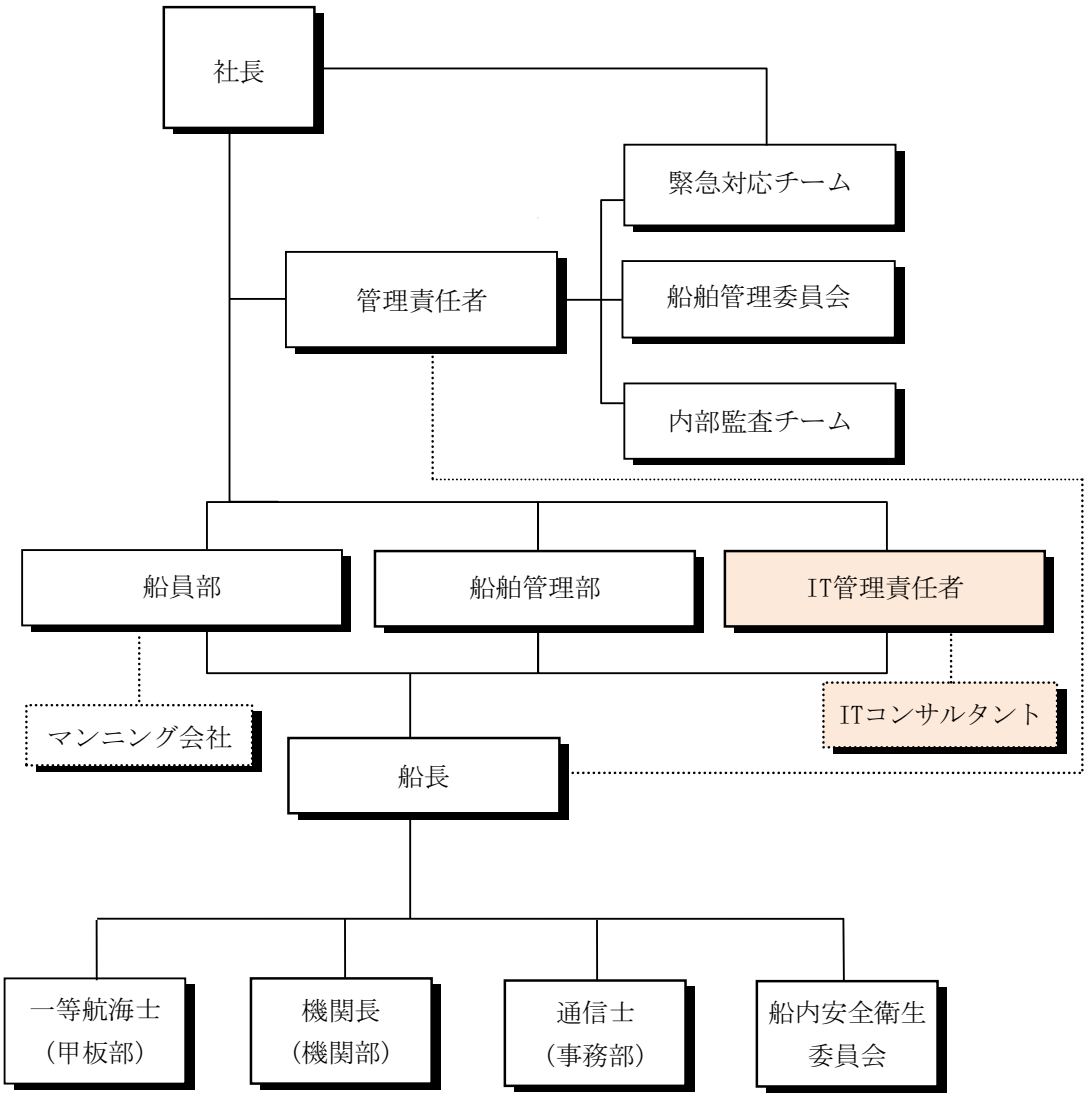
(省略)

2. 組織図

SMS 文書番号 No.： **章番号：**

作成者：管理責任者 **承認者：**

件名：組織図



3. IT システム管理規程

SMS 文書番号 No.： **章番号**
作成者：管理責任者 **承認者：**
件名：ITシステム管理規則

1. 目的

この規則は、サイバーリスクへの潜在的な対応を含む、会社および本船ITシステムの適切なSMSの実施に向けた、システムの配置ならびに管理を規定するものである。

2. 適用

この規則は、会社ならびにすべての管理船舶に適応する。

3. 参照規則

SOLAS XI-2
MSC-FAL-1/Circ.3

4. 定義

4.1 ITシステムとは
「IT システム」とは、あらゆるオペレーションに使用されるコンピュータベースのシステムを意味し、パッケージ化された機器全体、または PC にインストールされたソフトウェアであると言える。コンピュータを用いたあらゆる装置、機器、サービスの総称とし、また同時にそれらは「IT システム」を構成する一部と定義される。
4.2 サイバーリスクとは
「サイバーリスク」は、IT システムに障害または悪影響を与え、ひいては組織の信頼に関わるような、業務の混乱や経済的損失を引き起こす潜在的要因となり得る。サイバーリスクには、外的要因（コンピュータウイルス、トロイの木馬ウイルス、ネットワーク攻撃など）と内的要因（不具合、操作ミス、システムバグなど）がある。
4.3 ITインシデントとは
「IT インシデント」とは、実際にまたは潜在的に、IT システムに被害をもたらす事件の発生であり、IT システムに関与するすべての不具合や不適合を含む。

4.4　サイバーリスク管理とは

「サイバーリスク管理」とは、サイバー関連リスクを洗い出し、分析し、評価し、また会社の費用と恩恵を考慮しながら、そういったリスクを許容レベルに改善するべく、受け入れ、回避し、除去または軽減する手順である。

5. 要件

5.1　ITスタンダード設計

SMS の円滑かつ効果的な実施のために、会社は IT スタンダードを策定し、適宜、船陸ともに、IT システムを構築する必要がある。IT スタンダードは、「IT スタンダード設計記録」に記録、IT 管理責任者はその改善を毎年見直す必要がある。詳細は、「IT システム管理手順」を参照。

5.2　ITシステムの操作

管理責任者や船舶管理部上長の監督のもと、IT管理責任者は、特定のITシステムとネットワークシステムを適切に統合し、関係者を指揮監督して、ITスタンダードやメーカーのマニュアルに従いながらITシステムを操作しなければならない。

5.3　ITシステムの洗い出し

5.3.1　IT管理責任者は、「ITシステムリスト」を用い、船陸ともに、すべてのITシステムの洗い出しをする必要がある。

5.3.2　IT管理責任者は、各ITシステムに対するサイバーリスクのリスク評価を実施し、必要に応じて、対策を講じる必要がある。

5.3.3　リスク評価時に、ITスタンダードに関し、既にリスクアセスメント済のシステムはリスクアセスメントから除外できる。

5.3.4　ITシステムの追加、交換、または廃止が行われた場合、IT管理責任者はその変更部分に対し、リスク評価を再実施しなければならない。

5.4　ITシステムの保守対応

ITシステムの適切な運用のために、IT管理責任者は、関連するソフトウェアは当然のこと重要な要素を含んだITシステムの定期的な保守計画を構築する要がある。保守計画においては、次の要因を組み込むこと。

(1) 各ITシステムベンダーが指定するメンテナンス作業
(2) 小規模なソフトの更新
(3) データのバックアップ操作

(4) 各ITシステムの状態確認

IT システムのメンテナンスの際には、「船体、機械および機器の保守に関する規則」を参照すること。

5.5 ハードウェアの取り替え

5.5.1 耐用年数によって、ハードウェアの取り替えを行う。

5.5.2 IT管理責任者は、以下の要因を考慮し、ハードウェアの取り替えを計画する必要がある。

(1) ハードウェアベンダーからの推奨
(2) 各ITシステムの状態報告
(3) サイバーリスクを許容する新しいハードウェアによる改善

5.5.3 交換計画時は、以下の運用を含めなくてはならない。

(1) 劣化による対象PCの取り替え
(2) 劣化による周辺機器の取り替え
(3) サイバーリスクに対する新しい対策を備えたハードウェアへの取り替え
(4) ITシステムの適切な操作に必要と考えられるハードウェアへの交換

5.6 ITシステムのファームウェアまたはソフトウェアのバージョン管理

5.6.1 IT管理責任者は、ITシステムのファームウェアまたはソフトウェアのバージョン一覧を管理する必要がある。

5.6.2 アップデート版がリリースされている場合、出来るだけ最新版を使用すること。

5.6.3 但し、大幅なアップデートは、他のITシステム間の互換性や接続性に影響を与える可能性がある。その場合、更新前に、IT管理責任者は十分な確認とリスク評価を実施しなければならない。

5.6.4 IT管理責任者は、アップデートの大小の度合いを適切に判断する必要がある。

5.7 ITシステムのインシデントの取扱い

5.7.1 IT管理責任者は、船陸ともに、ITシステムに関するインシデントを処理および解決することを求められている。

5.7.2 IT管理責任者は、サイバーリスク許容の改善を念頭に、将来的な分析のために事故の記録を残す必要がある。

5.7.3　もしインシデントが重大であると見なされる場合、IT管理責任者は、「緊急対応策に関わる規則」に則り、管理責任者に報告しなければならない。
5.7.4　重大なインシデントの解決後、IT管理責任者は、再発防止に向けてリスク調査を実施する必要がある。
5.7.5　「ITシステムリスクアセスメント手順」もまた参照すること。

5.8　ITシステム運用に関する教育と訓練

5.8.1　IT管理責任者は、会社のSMSに携わるすべての関係者に対してITシステムおよびサイバーリスクの十分な理解を得る必要がある。
5.8.2　IT管理責任者は、ITシステム運用に関する適切な教育や訓練を計画しなければならない。
5.8.3　その教育・訓練計画は、「教育や訓練に関する規則」を参考に実施される。
5.8.4　IT管理責任者は、感染防止のために、新たに発見されたサイバーリスクについて、関連部署及び管理船舶へ遅延無く連絡する。

5.9　ITシステムのデータ管理

5.9.1　IT管理責任者は、ITシステムで運用されているデータを適切に管理しなくてはならない。
5.9.2　データ管理は、次の要因を考慮する。
(1) 有効性　　データは、適切なタイミングで使用できる
(2) 整合性　　データの損失や改ざんを防止すること
(3) 守秘義務　データは、権限のない第三者へ漏洩することはない
5.9.3　IT 管理責任者は、データの知的財産の所有権について明確にする必要がある。
5.9.4　船舶管理が移転する場合、IT 管理責任者は、「IT システムリスト」を参照の上、データを修正または削除しなければならない。

5.10　未知のサイバーリスクを監視すること

5.10.1 IT管理責任者は、未知のサイバーリスクの発見に努める必要がある。
5.10.2 船長または会社の各部門の担当者は、新しく洗い出されたサイバーリスクについて、IT管理責任者に知らせる必要がある。

5.11　ITシステムに関する管理の見直し

5.11.1 IT管理責任者は、見直しの際に、次の情報を安全管理委員会に提出する。

(1) ITインシデントの分析報告書
(2) 新たに発見されたサイバーリスクやリスク評価の報告書
(3) IT分野のトレンド情報
(4) ソフトウェアとハードウェアの最新情報
(5) リスク評価とITスタンダードの改訂計画
(6) リスク評価とITシステムリストの改訂計画

5.11.2 管理責任者は、これらの情報を調査し、「内部監査および管理の見直しに関する規則」を参照し、IT 管理を見直す必要がある。

5.12 ITのコンサルタントや専門家との契約について

5.12.1 インターネットに接続し、TCP/IPを用いたITシステム操作は、ITに関する高い知識と深い経験が求められる。

5.12.2 IT管理責任者を補佐するために、会社は外部の船舶ITシステムのコンサルタントや専門家と契約することがある。

6. 対応する手順書

ITシステム管理手順
ITシステムリスクアセスメント手順

7. 適応する記録

船会社と船舶：
ITスタンダード設計記録
ITシステムリスト
ITシステムリスクアセスメント記録
船体、機械および機器の関する保守計画書

4. IT システム管理手順

SMS 文書番号 No.： **セクション番号：**
作成者：管理責任者 **承認者：**
件名：ITシステム管理手順

1. 適用範囲

この手順書は、船陸ともに、ITシステムの管理の指針を定義しており、会社ならびに会社の管理船のすべてに適用する。

2. 参考文献

ITシステム管理規則

3. ITスタンダード設定手順

3.1 IT管理責任者は、「ITスタンダード設計記録」を用いてITスタンダードを設計し、ITシステムの統合を標準化することが求められる。

3.2 ソフトウェアとハードウェアの接続時の問題を防ぐにあたり、次の要素を検証する必要がある。
(1) 互換性
(2) 交換性
(3) 競合
(4) システムの応答速度

3.3 IT管理責任者は、本船および会社のITスタンダードを準備する。

3.4 IT管理責任者は、ITシステムを次のように分類する必要がある。

会社カテゴリー	故障時の影響度合い
A	商船運航に直接悪影響を与えるおそれのないシステム
B	商船運航にゆくゆくは影響を与えるおそれのあるシステム
C	商船運航に直ちに影響を与えるおそれのあるシステム

3.5 カテゴリーBとCについて、 IT管理責任者は、これらが持続して稼動するシステムを確保するための具体的な対策を講じなければならない。

3.6　また、船舶管理者は、ClassNKテクニカル・インフォメーションNo.TEC-1145にて定義されたITシステムを分類する必要がある。

分類	故障時の影響度合い
I	故障が人体及び船体への危険並びに環境への脅威に帰結するおそれのないシステム
II	故障が人体及び船体への危険並びに環境への脅威にゆくゆくは帰結するおそれのあるシステム
III	故障が人体及び船体への危険並びに環境への脅威に直ちに帰結するおそれのあるシステム

3.7　船舶管理者は、ITスタンダードに関してリスクアセスメントを実施する必要がある。

4. ITシステムのリスク評価手順

4.1　IT管理責任者は、ITシステムリスクアセスメント記録を用いて、ITシステムにて洗い出されたリスクについて、リスクアセスメントを実施することが求められている。

4.2　複数のITシステム間で接続があった場合、接続のリスクも検証する必要が出てくる。

4.3　リスクごとに、次の要因を評価しなければならない。

(1) 可能性
(2) 頻度
(3) 損害

4.4 リスク評価の結果として、次のオプションが選択される。

(1) リスク許容
(2) 措置が必要
(3) 追って要再評価

4.5　対策が求められる場合、IT管理責任者は対策を講じ、管理責任者の承認を得た上で実施する必要がある。

4.6　リスク評価にはITの高度な知識と経験が求められるため、ITのコンサルタントや専門家の助言が得られると望ましい。

5. ITスタンダードの見直し手順

5.1 IT管理責任者は、毎年、ITスタンダードを見直す必要がある。

5.2 ITスタンダードにて、改訂、加筆、削除などの変更が行われた場合、IT管理責任者はその変更箇所についてリスク評価を実施しなくてはならない。

5.3 たとえ変更が生じなくても、IT管理責任者は、依然として次の要因を考慮し、リスク評価の実施しなければならない。

(1) 運航環境や要件の変更
(2) IT技術の改善
(3) 新しいサイバーリスクの動向

5.4 ITスタンダードの更新は、管理責任者の承認を要する。

5.5 ITスタンダードの更新が承認された場合、IT管理責任者は、船陸ともに、それぞれのITシステムのアップデートを計画すること。

6. 新規の管理船舶に対するITシステムの整備

6.1 IT管理責任者は、「ITシステム構築のためのガイドライン」及び、ITスタンダードを参考に、本船ITシステムを統合しなければならない。同様に、「ITシステムリスト」に記録する必要がある。

6.2 IT管理責任者は、ITシステムリスクアセスメント記録を用いて、各ITシステムのリスク評価を実施する必要がある。

6.3 ITスタンダードでも、既にリスクアセスメント済の.ITシステムであれば、この部分のリスクアセスメントから除外できる。

6.4 また、もしその.ITシステムが、ClassNKテクニカル・インフォメーションNo.TEC-1145において、分類II及びIIIのアイテムでスタンドアロン利用のものも、リスクアセスメントから除外が可能である。これらのシステムは、システムベンダーによって評価されなければならない。

6.5 IT管理責任者は、保守計画以外に次の課題を用意する必要がある。

(1) システムベンダーから指示を受けるメンテナンス作業
(2) IT管理責任者から承認されたソフトウェアやファームウェアの小規模な更新
(3) データのバックアップ
(4) 状態の確認

6.6 これらの準備は、管理責任者に承認されなければならない。

7. 船舶管理の終了によるITシステム取扱手順

7.1 IT管理責任者は、「ITシステムリスト」を参照に、各本船ITシステムのデータを修正または削除する必要がある。

8. ITシステム改定手順

8.1 ITシステムの追加、交換、または廃止といった変更が計画された場合、IT管理責任者は次の要因を確認しなければならない。
(1) 互換性
(2) 交換性
(3) 競合性

8.2 また、IT管理責任者は、ITシステムの新しい接続のリスク評価も実施する必要がある。

8.3 リスクや問題が発見された際は、IT管理責任者は、新システム統合の運用や改定の延期といった対策を準備すること。

8.4 最終決定は、管理責任者に承認されなければならない。

9. ITインシデントの取扱い手順

9.1 IT管理責任者は、船陸ともに、発生したITインシデントの処理に当たること。

9.2 以下の状況下において、IT管理責任者は、管理責任者に重大なインシデントとして報告する義務がある。
(1) インシデントが、船の安全航行に直接影響を与える可能性がある場合。
(2) または、インシデントが、会社外の経済的損失を発生させる可能性がある場合。
(3) あるいは、解決の遅れが状況（1）または（2）を引き起こす可能性がある場合。

9.3 重大インシデントの場合、管理責任者は、「緊急対策に関わる規則」に則り、緊急対応チームを設置し対処することが求められる。

9.4 管理責任者は、ITコンサルタントやITの専門家に、必要に応じ、連絡できる。

9.5 「ITシステムリスクアセスメント手順」を参照。

10. 関連のフォームや情報など

ITシステム構築のためのガイドライン
ITシステムリスクアセスメント手順
ITスタンダード設計記録
ITシステムリスト
ITシステムリスクアセスメント記録
船体、機械および機器の関する保守計画書

付録

ITシステム統合のためのガイドライン

対象PC

(1) 対象PCモデルの選択時には、次の点を考慮すること。
  (a) ITシステムを運用するのに十分なCPU、電力、メモリ、HDD容量
    特に、セキュリティソフトウェアはこれらのリソースを必要とする
  (b) 船上で操作するにあたり、十分な信頼性を持つPCモデル
(2) 言語モデルは、ITシステムに影響を与える可能性がある。IT管理責任者は、PCが異なる国々から供給されているのかどうかを確認する必要がある。

OS

(1) 必要なセキュリティアップデートを適用するために、出来れば「自動更新機能」をONにしておく必要がある。
(2) しかしながら、OSの大幅なアップデートは、他のITシステムや周辺機器に影響を与える可能性もある。IT管理責任者が、OSのバージョン更新を決定した場合、十分な検証とリスク評価が必要となる。

基本的なソフトウェア

(1) 「基本的なソフトウェア」とは、MS-OfficeやPDFリーダーといった各ITシステムのシステム要件となるソフトウェアである。
(2) 基本的なソフトウェアの大幅なアップデートは、関連するITシステムに影響を与える可能性がある。したがって、IT管理責任者が、基本的なソフトウェアのバージョン更新を決定した場合、十分な検証とリスク評価が必要となる。

ソフトウェアアプリ

(1) すべてのアプリケーションソフトウェアは、IT管理責任者が、インストールを行う前にITスタンダード環境で検証する必要がある。
(2) アプリケーションソフトに通信機能が備わっている場合は、機能の詳細（通信ポート、送信先IPアドレスなど）を明確にしなくてはならない。ソフトウェアの通信の詳細が開示されていない場合、そのソフトウェアは適用外とする。
(3) アプリケーションソフトは、他のアプリケーションと競合する可能性がある。競合を避けるために、IT管理責任者は、導入前に十分な検証を実施すること。

ウイルス対策ソフト

(1) ウイルス対策ソフト（またはセキュリティソフトウェア全般）は、使用している業務用のすべてPCにインストールする必要がある。
(2) IT管理責任者は、ウイルス対策ソフトを作動させておくために、定義ファイル（またはパターンファイル）を更新する適切な方法の整備が求められる。
(3) 特に、海上のインターネットにアクセス可能な船舶では、「オンラインアップデート機能」が必要となる。

情報通信基盤 （通信インフラストラクチャ）

(1) 通信の信頼性を確保するためには、2種類以上の情報通信基盤を持つことが望ましい。
(2) 本船のITシステムは、特定の通信インフラストラクチャの影響を受けない「オープンシステム」として動作することが望ましい。本船ITシステムは通信から切り離しておく必要がある。
(3) 最新のサイバーリスクをコントロールするために、OSとアプリケーションのバージョンを自動で更新することは非常に重要である。衛星を経由して「自動更新」が不可能な船舶の場合、4Gなどの陸側通信を活用する。

船内ネットワーク (LAN)

(1) 船舶ネットワークは、各ITシステムが適切に動作できるように設計する必要がある。
(2) 船舶ネットワークは、複数のサブネットワークに分離し、パケット通信を管理する。
(3) 以下のITシステムは、通信量の大きさから、サブネットワークに分離されることが望ましい。
    (a) 乗組員福利のためのインターネット接続
    (b) CCD監視カメラシステム
(4) その重要性を識別したITシステムでは、通信の信頼性を確保するために、システムを独立したサブネットワークに配置する必要がある。
(5) 乗組員福利ネットワークの場合、船内Wi-Fiアクセスポイントを設置することが望ましい。それにより、乗組員は各自のプライベート端末の接続が可能となる。ネットワークの競合を避けるため、乗組員のネットワークにイーサネット接続を提供しないこと。

周辺機器について

(1) IT管理責任者は、LANに接続された全ての本船の周辺機器（ポート、送信先

IPアドレスなど）の通信機能の詳細を明確にする必要がある。通信の詳細が開示されていない場合、その機器は採用しないものとする。

乗組員のプライベート端末とプライベートインターネット接続

(1) 多くのサイバーリスクは、乗組員のプライベート端末や「港内のレンタル4G」などのプライベート接続に起因する。

(2) このような状況を整備するためには、IT管理責任者は、次のような適切な対策を講じる必要がある。
   (a) 乗組員に対して、十分なITリテラシーを養うよう、訓練や教育する
   (b) 本船業務用ITシステムとプライベート端末の管理方針の違いを区別する
   (c) 乗組員のプライベート端末やインターネット接続に起因するこのようなサイバーリスクを遮断するための具体的な施策を練る

(3) より良い解決策のひとつは、正式に乗組員のための制御されたインターネット接続を提供すること、次にIT管理責任者は、このようなサイバーリスクの回避のため、適切なフィルタとサブネットワーク設定を配備する

SNSや個人のEメールへのアクセス

(1) 船員によるSNSや個人のEメールへのアクセスは、セキュリティリスクを伴いかねない。

(2) IT管理責任者は、どの船内情報を保護するべきかを洗い出す必要がある。

(3) IT管理責任者は、乗組員に、安全が保証されている情報の取扱い方法について訓練しなくてはならない。

ライセンスコンプライアンス(使用条件の遵守)

(1) IT管理責任者は、すべてのソフトウェアとハードウェアに適切なライセンスがあることを確認しなければならない

(2) 未知のサイバーリスクを回避するため、次のシステムは禁止されている
   (a) 違法コピー
   (b) 海賊版
   (c) 無許可修正を施したハードウェア
   (d) 不正なネットワークデバイス

ネットワークルータ

(1) 通信インフラストラクチャから独立したネットワークルータを設置することが望ましい。すると、船内ネットワーク(LAN)は、それに依存せずに操作が可能である。

(2) ネットワークルータには、複数の情報通信インフラストラクチャを切り替える機能が必要である。
(3) ネットワークルータには、内部ネットワーク通信を制御する機能も必要である。
(4) 制御されていない通信や外部からのサイバー攻撃を回避するために、不要なポートはフィルタ設定で閉じておかなければならない。

6. サイバーリスク管理の手順

SMS 文書番号 No.： **セクション番号：**
作成者：管理責任者 **承認者：**
件名：ITシステムリスクアセスメント手順書

1. 適用範囲

この手順書は、ITシステムのサイバーセキュリティインシデントへの対応に求められる対策を考案するためのガイダンスが規定されており、会社ならびに会社管理下にあるすべての船舶に適用する。

2. 参考文献

ITシステム管理規則

3. 権限と責任

3.1 管理責任者の監督のもと、船舶管理部門の上長は、船内ならびに陸上に拠点を置く組織のITシステムを含む、サイバーリスク管理の責任を持つ。

3.2 IT管理責任者の任務は、ITシステムの潤滑な運用、監督、監視、及びサイバーインシデントに対して遅延無く対応することである。

3.3 海上の船長は、ITシステムの潤滑な運用、監督、監視のほか、「不具合や不適合の管理手順書」に遵守し、あらゆる不具合や不適合、もしくは会社へのサイバーインシデントに関する報告を担う。

4. 手順について

4.1 脅威の洗い出し。IT管理責任者は、船舶管理部門の上長および管理責任者の指揮のもと、本船および会社に対する外部からのサイバーセキュリティの脅威を関係者全員に理解してもらい、また、不適切な使用と意識の欠如によって引き起こされる内部のサイバーセキュリティの脅威も理解させる措置を取る。

4.2 脆弱性の特定。IT管理責任者は、「ITシステムリスト」を参照に、直接的または間接的な通信リンク用い、会社および船舶システムのインベントリ

を立案する。また、これらのシステムを脅かすサイバーセキュリティの脅威と、既存の保護対策の能力と限界を理解することが求められる。

4.3 リスクの影響度を評価。IT管理責任者は、個人のセキュリティと安全の影響、または、悪用されている脆弱性との組み合わせ、および不適切な使用によって、外部からの脅威に悪用される脆弱性の可能性を評価、判断することが求められる。「ITシステムリスクアセスメント記録」のフォームが適用される。

4.4 保護対策および検出方法の開発。IT管理責任者は、船舶管理部門の上長および管理責任者の指揮のもと、保護対策を通して、脆弱性が悪用される可能性について何らかの対策を講じ、また、その悪用された脆弱性が与え得る潜在的な影響を軽減するための措置を取る。

4.5 緊急時対応策の策定。IT管理責任者は、「不具合や不適合の管理手順書」に従って、管理責任者の監督、承認をもって、脅威による影響を削減するための対応計画を策定する。

4.6 サイバーセキュリティインシデントに関する対応と復旧。上記の対応計画を用いて、サイバーセキュリティインシデントから復旧後、IT管理責任者は、対応計画の有効性の影響を評価し、脅威と脆弱性を再評価すること。

4.7 サイバーインシデントの調査。IT管理責任者は、船舶管理部門の上長および管理責任者の監督のもと、潜在的なサイバーリスクや過去の教訓をよりよく理解するためにサイバーインシデントを調査し、再発防止のために技術的で段階を踏んだ措置を策定していく。

4.8 ITシステムのサイバーインシデントへの対応。IT管理責任者は、「不具合や不適合の管理手順書」に従って、その脆弱性と影響を評価し、対応し、また最終的に安全とセキュリティを確保するための運用技術システムのメーカーと調整を行う。

5. 関連のフォームや情報など

ITスタンダード設計記録
ITシステムリスト
ITシステムリスクアセスメント記録

7. IT スタンダード設計記録

ITスタンダード設計記録

スタンダードタイプ:
記録日:
IT管理責任者:
管理責任者:

I. 対象PCの状態				**備考**
(1) ハードウェア(PC)				
	台数			
	PCのタイプ (ラップトップ/デスクトップ)			
	CPU			
	メモリー			
	HDD			
(2) ソフトウェア	**基本的なソフトウェア**			
	OS			
	マイクロソフトオフィス(バージョン)			
	マイクロソフトオフィス(アプリケーション)			
	アドビリーダー			
	ウイルス対策ソフト			
(3) ソフトウェア	**アプリケーションソフト**	**アプリケーション**	**供給者**	
(4) ネットワーク図	**PC設定の詳細**			
	PC設定の詳細			
II. 周辺機器				
(1)プリンター				
	レーザープリンター			
	＊台数			
	＊単機能または複合機			
	＊モノクロ/カラー印刷			
	インクジェットプリンター			
	＊台数			
	＊単機能または複合機			
	＊モノクロ/カラー印刷			
(2) スキャナー				
	＊台数			
	＊フラットベッド/スタンド			
NASセット				
	＊モデル			
III. ネットワーク				
(1) ルーター				
	ルーターのタイプ			
	供給者			
(2) サブネットワーク				
	サブネットワークの目的			
(3) 船内Wi-Fiアクセスポイント				
	Wi-Fiアクセスポイントの数量			
(4) ネットワーク図				
	ネットワーク図			

PC設定の詳細

	PC01	PC02	PC03	PC04	PC05	PC06
設置場所または主な用途						
設置場所(船橋、船長室など)						
PCのタイプ(デスクトップまたはラップトップ)						
主な用途(e-mail、SMS-MAIN、SMS-SUBまたはオフィスワーク)						
e-mail機能(メイン、サブまたは機能なし)						
LANの使用(はい/いいえ)						
ソフトウェア						
周辺機器						
レーザープリンター						
単機能, 複合機, モノクロ印刷またはカラー印刷						
インクジェットプリンター						
単機能、複合機、モノクロ印刷またはカラー印刷						
スキャナーの設置						
ドライバーインストール/スタンダードソフト/品質調整						
プリンター						
スキャナー						

ネットワーク図

ITシステムリスト

船名：＿＿＿＿＿＿＿＿＿＿＿＿

作成日：＿＿＿＿＿＿＿＿＿＿＿＿

作成者：＿＿＿＿＿＿＿＿＿＿＿＿　　管理責任者＿＿＿＿＿＿＿＿＿＿＿＿

1. アプリケーションソフト

カテゴリー		システム名	供給者	バージョン		データ			備考
クラス	会社名			No.	更新	プロパティ(属性・特性)	バックアップ	アクション	

2. ネットワーク

カテゴリー		システム名	供給者	バージョン		データ			備考
クラス	会社名			No.	更新	プロパティ(属性・特性)	バックアップ	アクション	

3. 航海計器

カテゴリー		システム名	供給者	バージョン		データ			備考
クラス	会社名			No.	更新	プロパティ(属性・特性)	バックアップ	アクション	

船舶ITリスクアセスメント報告書

船名 _____

作成日 _____

作成者 _____　　管理責任者 _____

案件名								
リスク発見日	リスク事象	リスク評価			評価	対策	対策実施日付	状況
		可能性	頻度	損害				

案件名								
リスク発見日	リスク事象	リスク評価			評価	対策	対策実施日付	状況
		可能性	頻度	損害				

案件名								
リスク発見日	リスク事象	リスク評価			評価	対策	開始日	状況
		可能性	頻度	損害				