JAPAN P&I CLUB　第42号 2018年5月

P&I ロスプリベンションガイド

編集：日本船主責任相互保険組合　ロスプリベンション推進部

サイバーリスクと サイバーセキュリティ対策

JAPAN P&I CLUB

P&I ロスプリベンションガイド

目　次

1. はじめに …… 1
2. 船舶通信とウイルス感染事例 …… 2
3. サイバーセキュリティ対策についての各船社の準備作業 …… 5
4. IT 管理責任者を選任する …… 10
5. 自社の IT スタンダードを制定する …… 11
6. 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 …… 13
7. SMS マニュアルに IT 管理文書を盛り込む …… 13
8. おわりに …… 14
9. 付録 …… 14

株式会社オルカ提供の文章やフォームの和訳

1. 組織規程 …… 15
2. 組織図 …… 16
3. IT システム管理規程 …… 17
4. IT システム管理手順 …… 22
5. IT システム統合のガイドライン …… 27
6. サイバーリスク管理の手順 …… 31
7. IT スタンダード設計記録 …… 33
8. IT システムリスト …… 36
9. リスクアセスメント記録 …… 37

◆ 当組合作成ポスター …… 38

1. はじめに

海上におけるサイバーリスクの脅威は日々増加しており、当組合でも「サイバーリスクとサイバーセキュリティ」と題したJapan P&I Newsを発行し、サイバーリスクに関する情報を提供しているところです。IMO（MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management）や世界の各海運団体等でもサイバーセキュリティ対策の必要性やガイドラインを紹介しており、海事分野におけるサイバーセキュリティの関心は急速に高まっているところです。
サイバーセキュリティ対策の必要性について組合員の皆様のご理解を深めて頂けるようこのたび本ロスプリベンションガイドを発行する運びとなりました。

1－1　サイバーリスクとP&I保険

古野電気（株）ご提供
次世代ブリッジシステム　Voyager

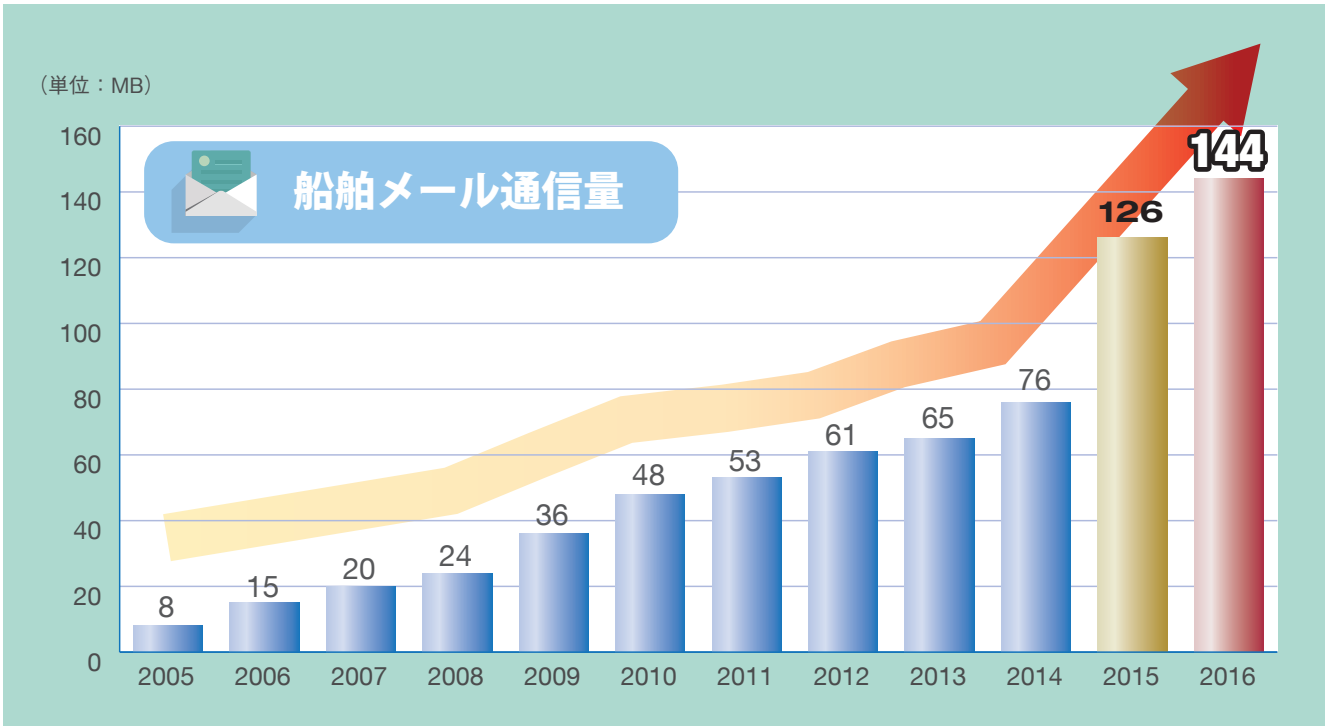
当組合の保険契約規定ではサイバーリスクを特定した規定はありませんが、もしサイバー攻撃や侵害によるクレームが起きた場合は現行の保険契約規定に則り通常通りにてん補の可否を検討します。サイバー攻撃が保険契約規定の第35条の「戦争」や「テロ行為」に該当しないと判断された場合、通常のP&I保険によるてん補の対象となりえます。
例えば、乗組員の個人PC、本船業務用のE-mail PCを経由して船内LANシステムにウイルスが感染してしまった、または本船で業務PCを許可なくUpdateしてしまった、または本船で乗組員が許可なく船内LANケーブルを繋ぎ変えた結果、航海用電子器機器や本船の推進設備に不具合が生じて、出港時に本船が港湾設備損傷を発生させてしまった場合などは、通常のP&I保険によるてん補の対象となります。

P&I保険の対象となりませんが、相談のあった事例として、メールハッキングにより船用品代金を誤送金してしまった事例や、本船乗組員個人PCに保管されていた動画がテロリズムを彷彿させるとして、乗組員が当局で取り調べを受けて、本船の予定が遅延してしまった事例、また本船をアレストするとして事実無根の金銭要求をする脅迫メールが本船に送信された事例など、P&I事故までには発展しない事例が報告されております。

2. 船舶通信とウイルス感染事例

2－1 船舶通信

航行区域に従って船舶に搭載を要求される GMDSS（Global Maritime Distress and Safety System）機器を除くと、本船には V-SAT、Fleet Xpress、FBB、Iridium や 4G 回線を利用したインターネット、E-mail、電話、Fax 等の船舶通信機器が多く利用されております。これらの船舶通信機器は、単に船陸間のコミュニケーションとしてのツールだけではなく、ウェザールーティング・海図改補・PMS（Planned Maintenance System）といった現在本船の運航において欠かせない機器です。
それに伴い船舶メール通信量も増加しています。グラフ 1 は、過去 12 年間の月あたりの船舶メール通信量を現したグラフです。2005 年と比較して 2016 年には通信量は約 18 倍に増加しています。



グラフ 1　過去 12 年間の月当たりの船舶メール通信量

２－２　ウイルス感染事例

一方で、船舶通信量の増加とともに船舶 PC や船舶システムにウイルス感染する事例が増加し、ウイルス感染経路も変化してきました。

2000 年頃までは、船舶のウイルス感染はメールプロバイダ側でブロック、また船内ネットワークは、外部ネットワークとそもそもつながっていない船舶が多かったため、乗船する人間・船員がウイルスファイルを物理的に持ち込んでしまう事例がほとんどでした。

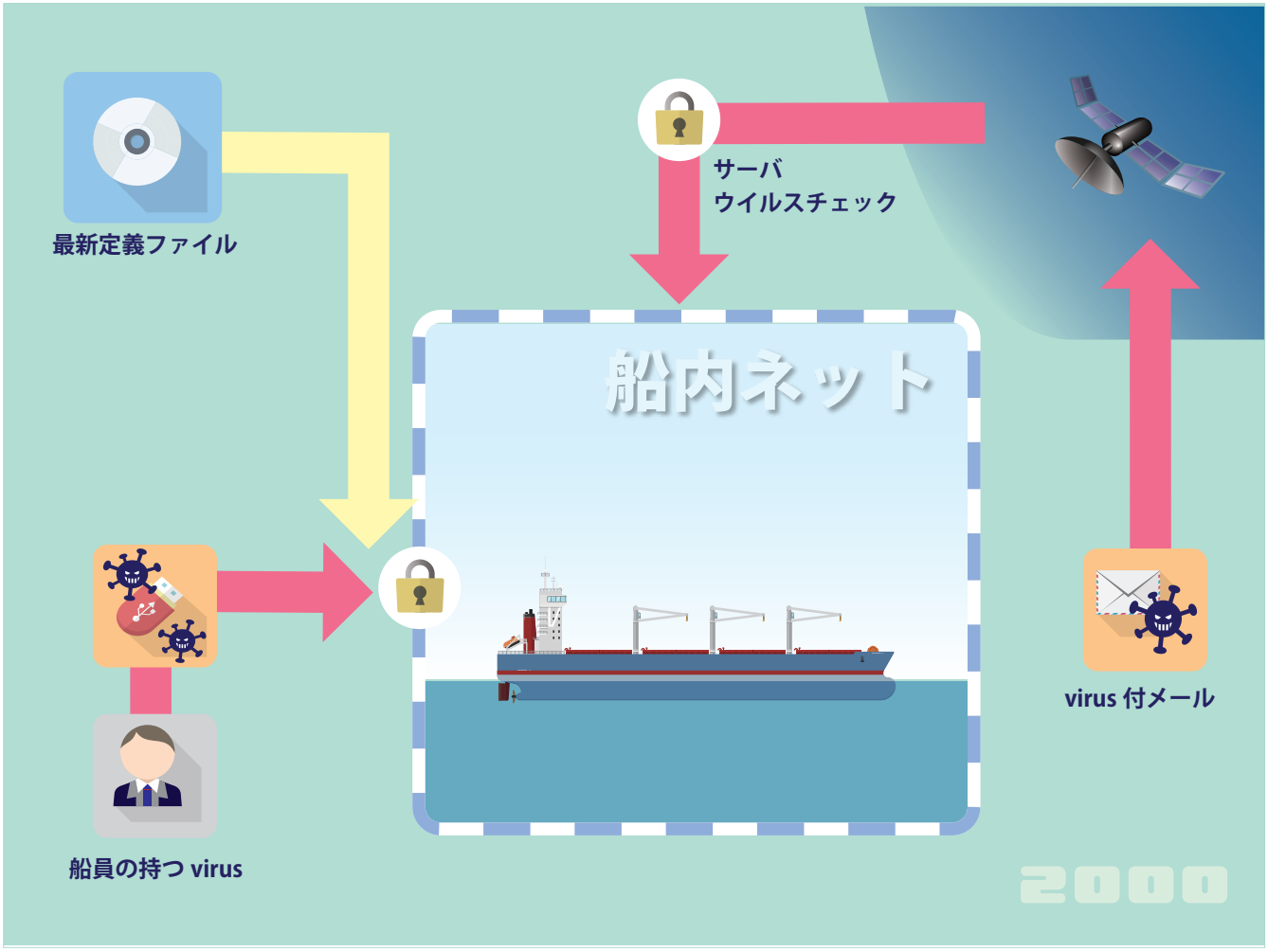


図 2. 2000 年頃

2010 年頃より、乗組員が寄港時に使用する 3G/4G 通信により最新のウイルスが流入して船舶ウイルス感染、その結果としてメールが不通になってしまうという事例が発生するようになりました。

図 3. 2010 年頃

違法コピーソフトの利用、違法ダウンロードサイトの利用といった行為が、結果として最新のウイルスが多く集まるような状況を作ってしまっているのも一因と考えられます。

この船舶通信機器とそれにつながる船舶 PC 及び航海電子機器や推進装置等が、サイバーセキュリティ対策を検討する上で必要不可欠であることは想像できますが、具体的にどのようなアプローチでリスクアセスメント、SMS（Safety Management System）改訂又は SSP（Ship Security Plan）改訂の検討のために着手して良いか分からないという声も聞かれます。

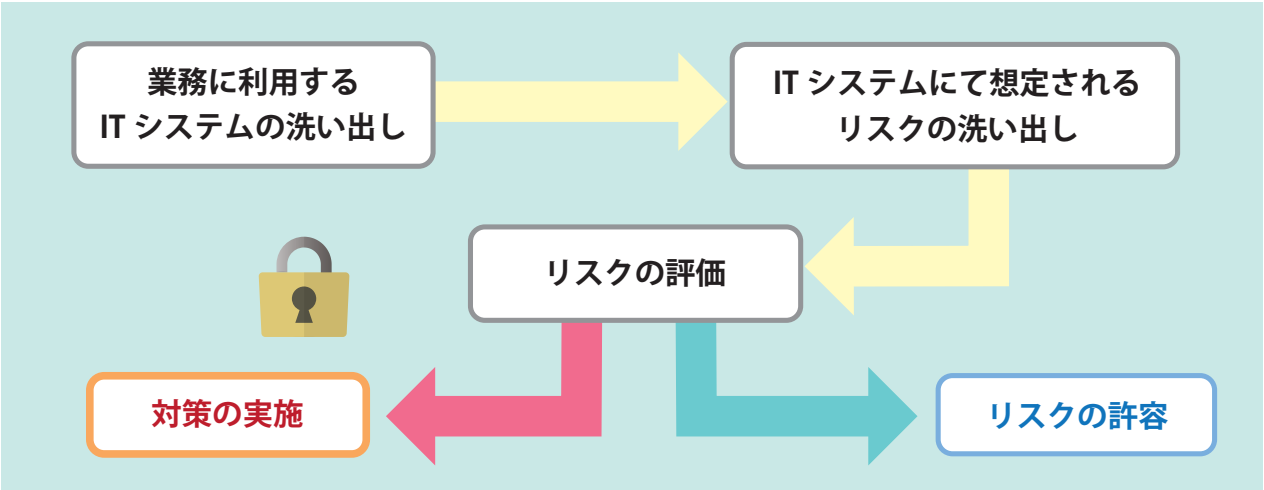
本ガイド後半では、船舶 IT 分野で実績のある株式会社オルカが、サイバーセキュリティ対策のリスクアセスメントのアプローチ手法を用いて MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management を想定した SMS の雛型を紹介しています。

3. サイバーセキュリティ対策についての各船社の準備作業

3－1　サイバーリスクを防ぐ考え方

サイバーリスクとはITシステムに障害または悪影響を与え、業務の混乱や経済的損失を引き起こす潜在的要因とここでは定義したいと思います。

ITシステムとは　業務に利用するコンピュータ（Information Technology）を用いたソフト、ハード、システム、機器、装置の総称とします。



3－2　ClassNK テクニカル・インフォメーション No. TEC-1145 の解説

IACS はコンピュータシステムのセキュリティ対策の重要性に鑑み、船舶で使用されるコンピュータシステムに対する関係者の役割、並びに、コンピュータシステムに用いるソフトウェア及びハードウェアのセキュリティ対策及びソフトウェア変更手順等の品質管理に関する要件を明確にすべく、IACS 統一規則E22（Rev.2）が2016年6月に採択されました。

これに伴い2018年2月28日に発行されたClassNK テクニカル・インフォメーション No.TEC-1145 にて

関連規則及び検査要領を改正した旨の案内がありました。
ClassNK テクニカル・インフォメーション No.TEC-1145 において、本船に搭載される自動制御又は遠隔制御を行う各ソフトウェア及びハードウェアに対して、それらの故障が与える影響度によって分類され、造船所、システムの統合者、供給者及び船主に責任と義務が区別されました。

鋼船規則検査要領 D 編附属書 D18.1.1 表 2.1 コンピュータシステムの分類

分類	故障時の影響度合い	システムの機能
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	― 情報収集又は管理業務に関するシステム
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	― 警報及び監視機能 ― 船舶の正常な操船及び居住状態を維持するための制御システム
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	― 推進及び操舵に関連する制御システム ― 安全システム

（No. TEC-1145 より抜粋）

分類Ⅲ

システム	具体的な機器及びシステムの例
推進システム	機関制御装置、機関遠隔制御装置、主ボイラ制御装置、CPP 制御装置、電気推進制御装置
操舵制御システム	操舵システム、旋回式推進システム
電源システム	発電機制御装置、電力変換装置（電気推進船等）
安全システム	火災探知装置、消火装置、浸水警報装置及び排水設備、船内通信システム、救命設備作動に関わるシステム
その他	自動船位保持装置、掘削装置

（No. TEC-1145 より抜粋）

分類Ⅱ

液体貨物移送制御システム	貨物制御装置（貨物制御盤、弁遠隔制御装置、緊急遮断装置）、再液化装置、イナートガス発生装置（窒素発生装置を含む）、油排出監視制御装置
燃料油操作システム	粘度制御装置、燃料油清浄機、燃料油こし器
船舶の安定及び浮揚制御システム	フィンスタビライザー、ジェットフォイル
推進システムの警報及び監視システム	機関警報監視装置（データロガーを含む）
その他	バラスト移送用弁遠隔制御システム、油水分離装置、油分濃度警報装置、廃油焼却炉、汚水処理装置、補助ボイラ制御システム、バラスト水処理装置、SOx/NOx スクラバー、NOx 排ガス再循環装置

（No. TEC-1145 より抜粋）

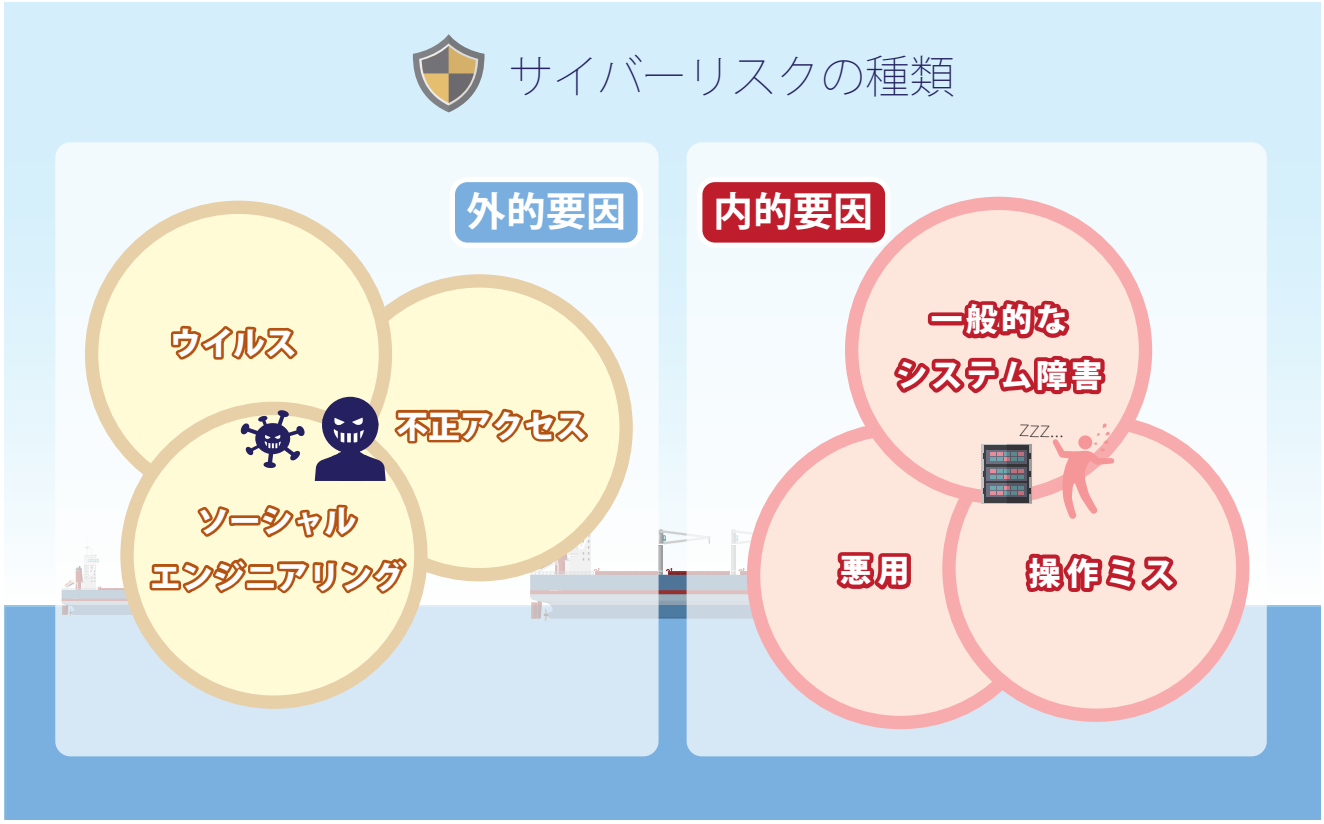
各コンピュータシステムのサイバーセキュリティ対策の責任の所在は各コンピュータシステムの供給者（Supplier）と定義されておりますが、システムを接続した場合は単体での運用では想定されないリスクが新たに発生するため、システムの統合者（System integrator）に責任が求められることになります。

船主及び船舶管理会社の役割は、各システムの供給者、造船所及び統合者よりコンピュータ使用機器一覧やリスク評価結果等の必要な情報を引き継ぐことであり、取り立てて何かを準備しなければならないということはありません。

ただし、将来の SMS 改訂（サイバーセキュリティ対策）において、「システムの統合者が一定の責任を負う」という概念は重要であり、分類 I に分類されるような船舶の業務用 PC、Loading Computer、V-SAT、FBB 等は、サイバーセキュリティ対策として船主または船舶管理会社によってリスク評価を実施しておく必要があります。

３－３　サイバーリスクの種類

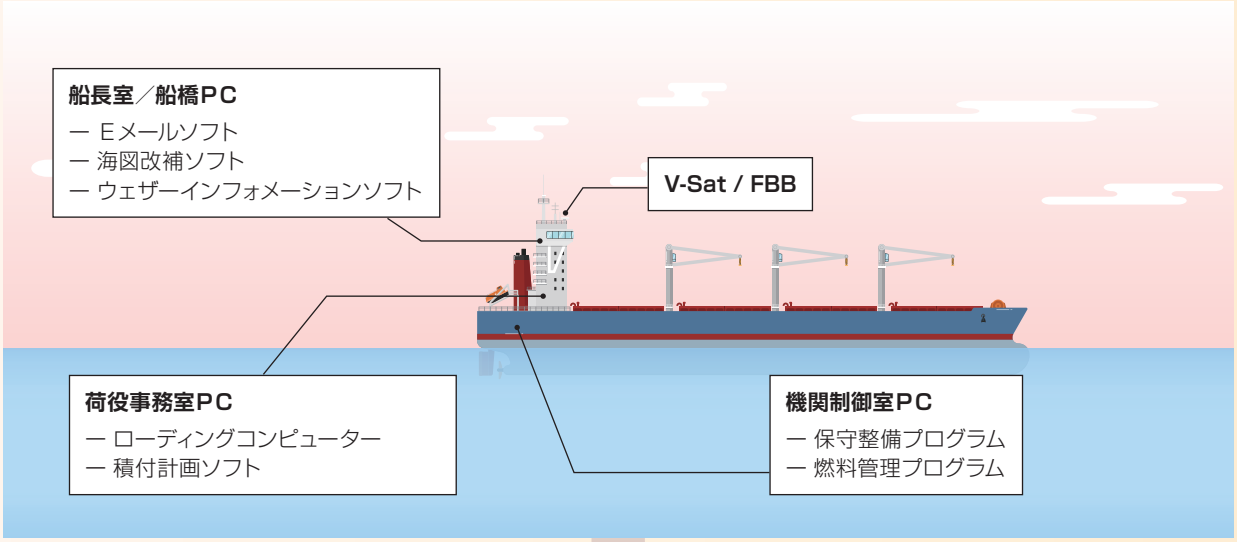
サイバーリスクというとシステムの不正アクセスやハッキングなど、外的要因が注目されがちですが、操作ミスや一般的なシステム障害といった内的要因も存在しているということを再度見つめなおす必要があります。



3－4　サイバーセキュリティ対策立案の流れ

1 IT システムの洗い出し

本船に搭載されている IT システムを洗い出し、リストアップする。



2 リスクアセスメントの実施

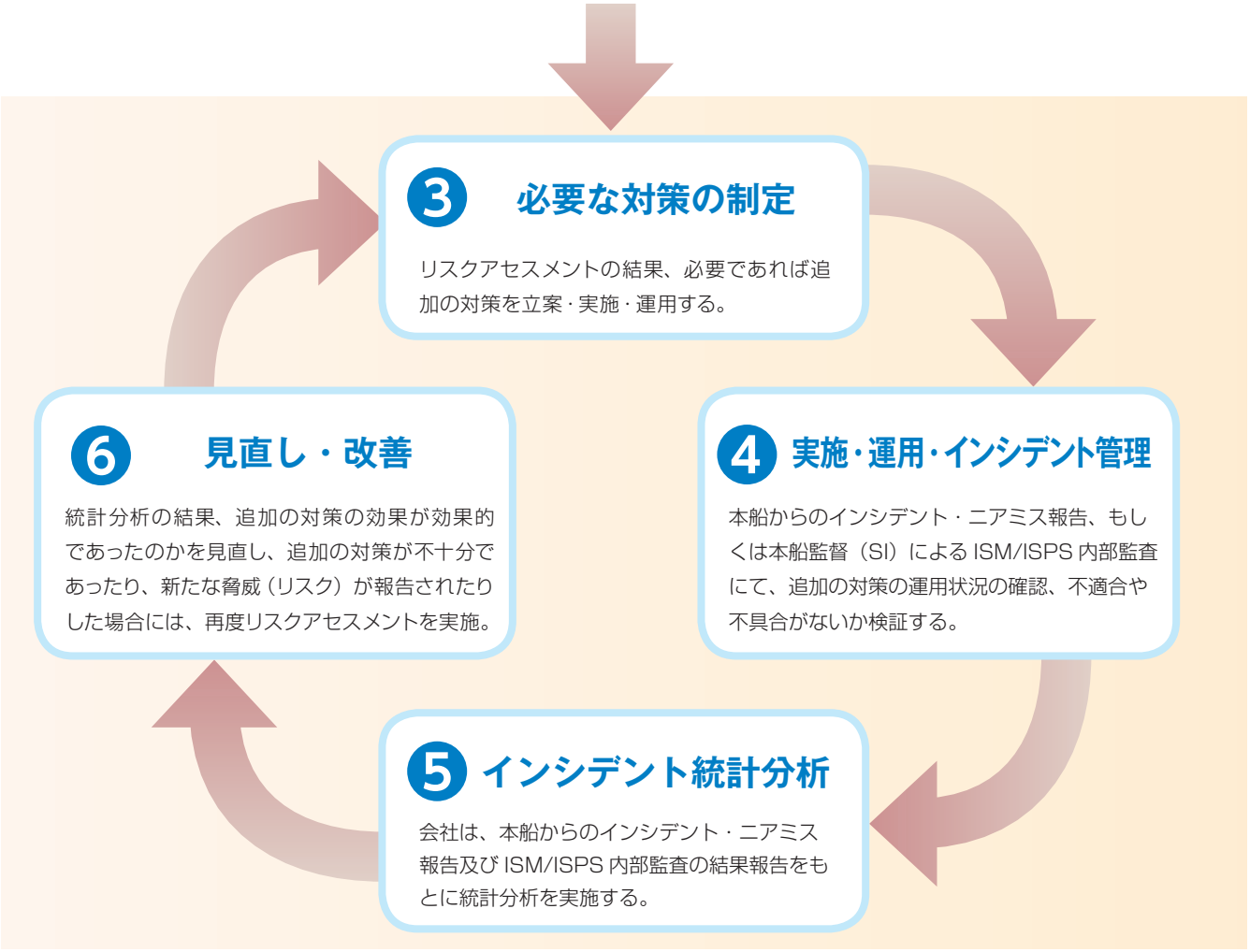
リストアップした IT システム毎に対して、起こる結果（損害）と頻度、既存の管理手法を検討しながらリスクアセスメントを実施する。

表 4　リスクアセスメント例

E-mail 通信

No.	シナリオ（Scenario）	可能性 (Possibility)	頻度 (Frequency)	損害 (Damage)	評価 (Evaluation)	対策 (Counter measures)	実施期日 (Due date)
1	船員個人 USB からのウイルスによるメールソフトの不具合	中（Middle）	中（Middle）	中（Middle）	追加の対策が必要	① SMS 教育手順追加 ②バックアップ PC 手配	2018 年 12 月
2	Firewall 未設置による、高額通信料金の発生	中（Middle）	高（High）	中（Middle）	追加の対策が必要	次港で技術者派遣し、FW 設置及び FBB 本体にフィルター設定	2018 年 12 月
3	船員個人 PC を直結されて業務通信を使用される	低（Low）	低（Low）	中（Middle）	リスク許容	リスクを許容するが、FBB フィルターの設定でこちらも改善される	N/A
4	衛星・地球局の不具合	低（Low）	低（Low）	中（Middle）	リスク許容	N/A	N/A
5	続く・・・						

リスクアセスメント及び SMS は、船員構成、運航する海域、船種及び管理会社により異なりますので、上記は一例となります。



❶…… 本船の IT システムを洗い出して、リストアップする。

❷ ❸ …… 本船上で特定していた危険作業や危険区域を既存の SMS で運用していたように、本船の IT システムを洗い出して、起こる結果（損害）と頻度、既存の管理手法を検討しながらリスクアセスメントを実施し、必要であれば対策を実施する。サイバーリスクを想定する上では、IT 分野のトレンドやシステムや機器の Type, Version といったことも考慮する必要があります。

❹…… 本船からのインシデント・ニアミス報告もしくは、本船監督（SI）による ISM 内部監査にて、追加の対策の運用状況の確認、不適合や不具合がないか検証する。

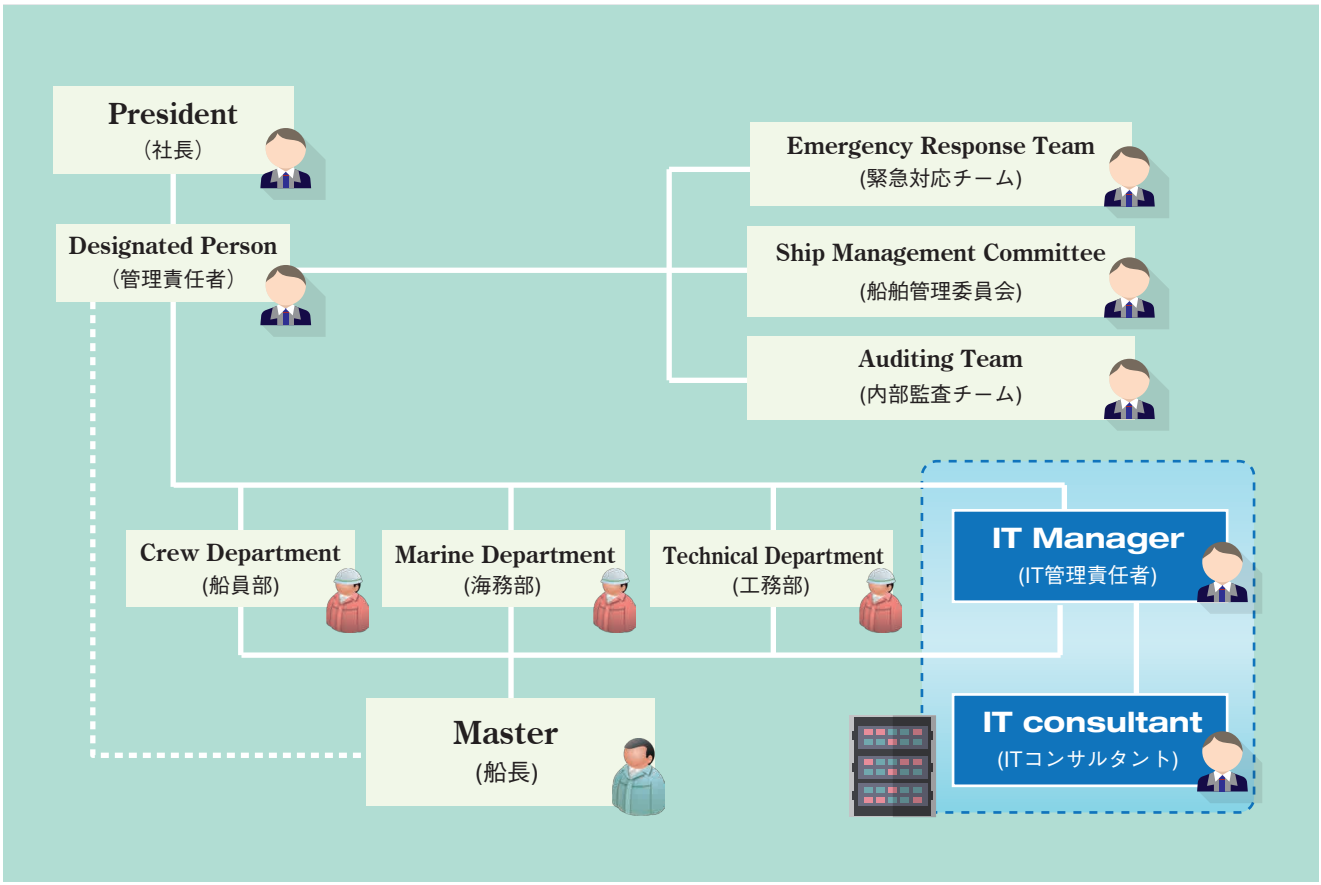
❺ ❻ …… 会社は、本船からのインシデント・ニアミス報告及び ISM 内部監査の結果報告をもとに統計分析を実施する。統計分析の結果、追加の対策の結果が効果的であったのかを見直し（マネージメントレビュー）、追加の対策が不十分であったり、新たな脅威（リスク）が報告されたりした場合には、再度リスクアセスメントを実施の上で、必要な対策を検討していく既存の SMS と同じ運用になります。

乗組員が会社で許可されていない USB メモリを、業務用 PC に挿入して使用した、または許可されていないソフトやプログラムを本船業務用 PC にダウンロードしていたといった事例が、ISM 上のインシデント・ニアミス報告として提出される時代になったと言えます。

また SMS と同時にサイバーリスクの外的要因となりうる訪船者に対応するために、特に寄港地において不特定多数の訪船者や港湾労働者が乗船する場合や、多くの研究者や作業者が乗組むような多目的作業船・海洋調査船等は、SSP も見直す必要性が出てくるかもしれません。

4. IT 管理責任者を選任する

サイバーセキュリティ対策を策定及び SMS へ取り込み、運用していくにあたり、IT 管理責任者を選任することが望ましいと思われます。今後、事故対応時の緊急対応や本船のシステム保守・導入に際して、ますます IT 管理責任者の役割と重要性は増してくるでしょう。また外部の船舶 IT システムの専門家に、相談できる体制をとっておくことも重要です。



5. 自社の IT スタンダードを制定する

管理船舶が複数隻ある場合、IT スタンダードを制定することで、運用及び管理手法（保守対応等）が統一できます。またトラブル発生時に IT スタンダードを制定していない場合と比べて対応が容易になります。

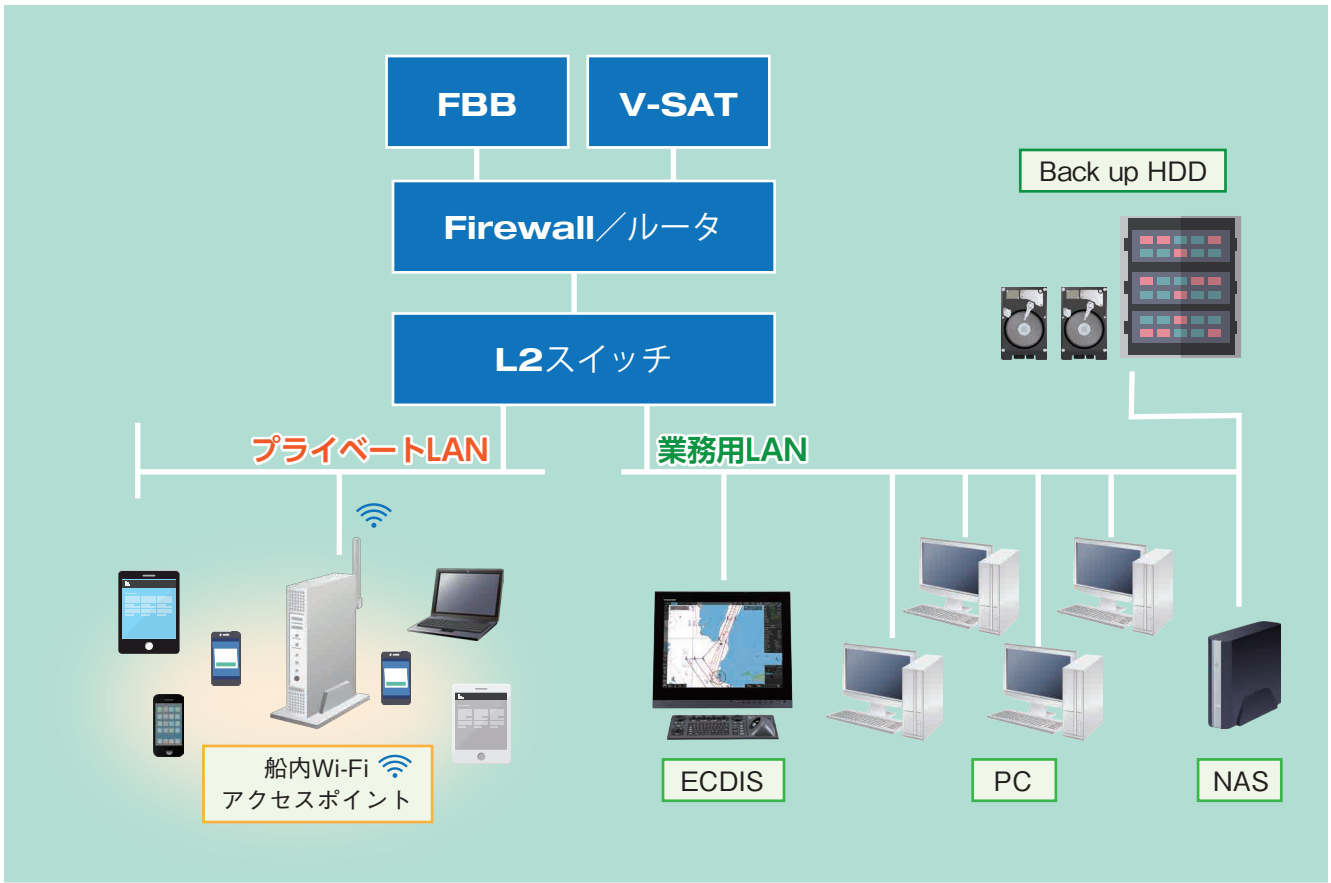


図 5. 船内 LAN の構築例

本船上の各 PC の仕様・ソフトウェア・用途を整理して置くことも重要です。PC 故障時に代替え PC を準備する、または新しいソフトウェアを追加するといった際に参考となります。

本船の PC 環境設計を記録しておく！

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			

表 7. ITスタンダード設計記録

6. 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

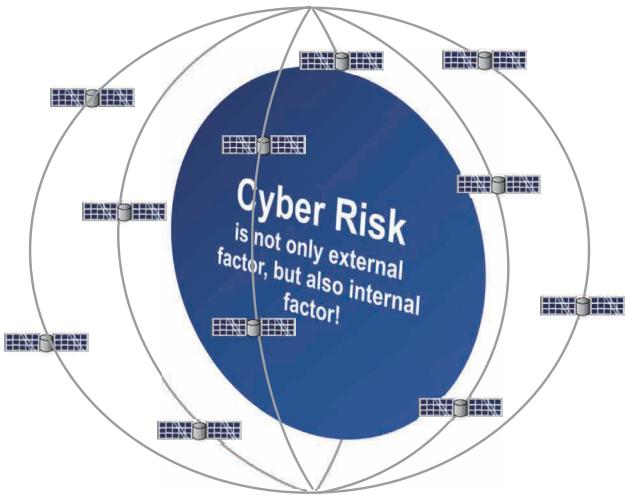
本ガイド３－４サイバーセキュリティ対策立案の流れで紹介している要領で制定した IT スタンダート（船内 LAN/PC 仕様）に関して、リスクアセスメントを実施します。
但し、既にリスクアセスメント済のシステムや、障害が発生しても直接業務に支障をきたさない IT システム、Class Category で II 及び III のアイテムで、スタンドアロン利用のものは、リスクアセスメントから除外できます。

7. SMS マニュアルに IT 管理文書を取り込む

各社においてリスクアセスメントを実施、SMS マニュアルに IT 管理文書を取り込んだ後に、重大な IT インシデントに関する船陸合同対応訓練やシミュレーションを一度実施することを推奨いたします。SMS マニュアルで策定したサイバーセキュリティ対応マニュアルや手順が効果的に機能していたか、陸上社員・本船乗組員は新しいマニュアルに習熟していたか等を見直す良い機会となるものと思われます

8. おわりに

サイバーリスクの脅威は船舶に限ったことではありませんが、航海中、外部からのアシストを受けられず、かつ堪航性が求められる船舶にとってはより一層のセキュリティ対策が必要です。
本ロスプリガイドを是非活用頂き、皆様のサイバーセキュリティ対策の立案の一助になれば幸甚です。
＜備考＞本ガイド内の資料と内容は、株式会社オルカ（http://www.orcajpn.co.jp/index.html）の協力を得て作成しています。



株式会社オルカ提供の文章やフォームの和訳

以下の文章やフォームは、当組合の WebSite（https://www.piclub.or.jp/lossprevention/guide）からも入手可能です。

株式会社オルカ提供の文章やフォーム

1. 組織規程 …… 15
2. 組織図 …… 16
3. IT システム管理規程 …… 17
4. IT システム管理手順 …… 22
5. IT システム統合のガイドライン …… 27
6. サイバーリスク管理の手順 …… 31
7. IT スタンダード設計記録 …… 33
8. IT システムリスト …… 36
9. リスクアセスメント記録 …… 37

◆ 当組合作成ポスター …… 38

参考文献 「ICS Bridge Procedure Guide Fifth Edition」

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。

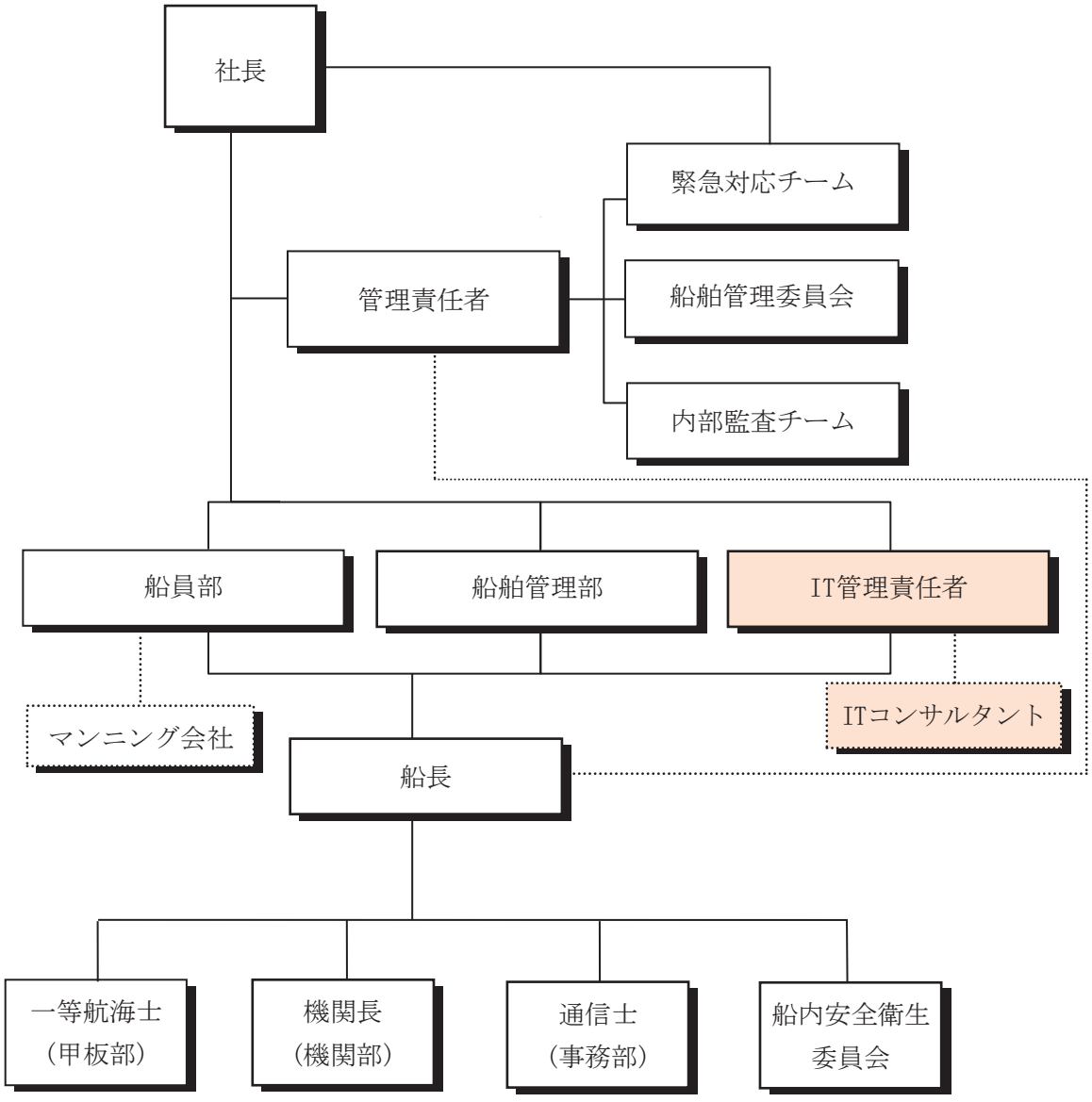
(省略)

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

5. IT システム統合のガイドライン

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 _____

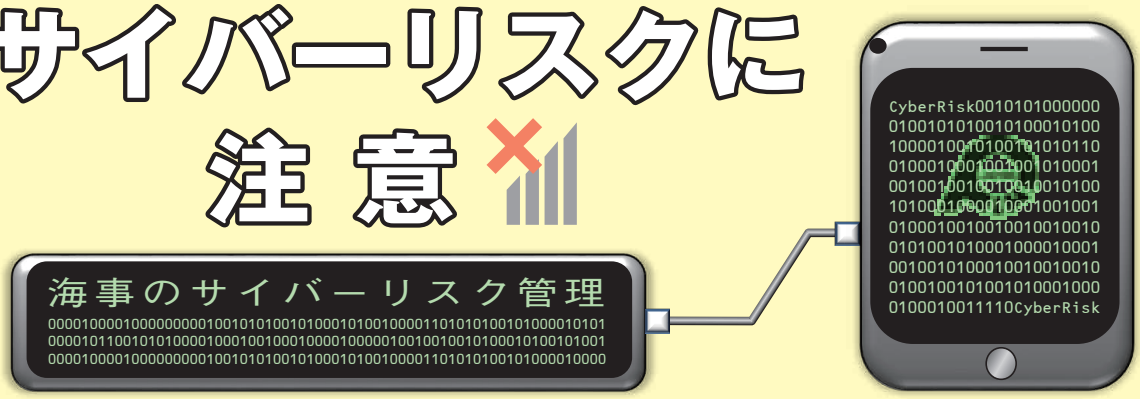
案件名								
リスク発見日	リスク事象	リスク評価			評価	対策	対策実施日付	状況
		可能性	頻度	損害				

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				

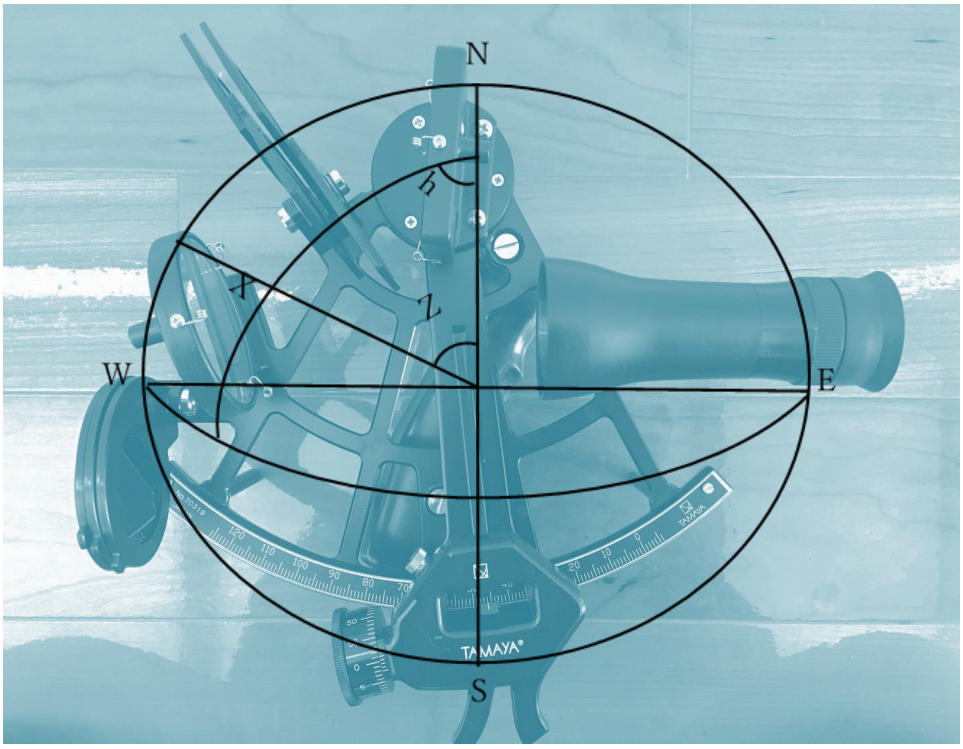
◆ 当組合作成ポスター

サイバーリスクに注意



もう一度、天文航法を検討？

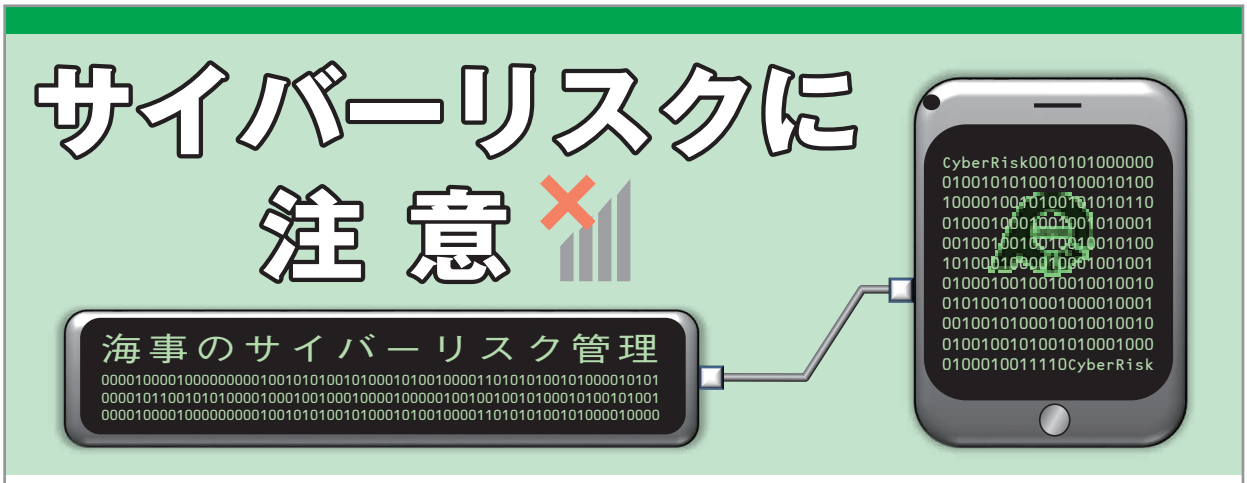
ECDIS 使用中に GPS(全地球測位システム)にシステム障害が生じた場合に、
代替手段を準備していますか？



ICS Bridge Procedure Guide(3.11.3 ECDIS 上の航海計画の監視)によれば、
特に適切な見張りの支障となるような場合、ECIDS への過度な依存は避けるべきとあります。

船 橋 掲 示

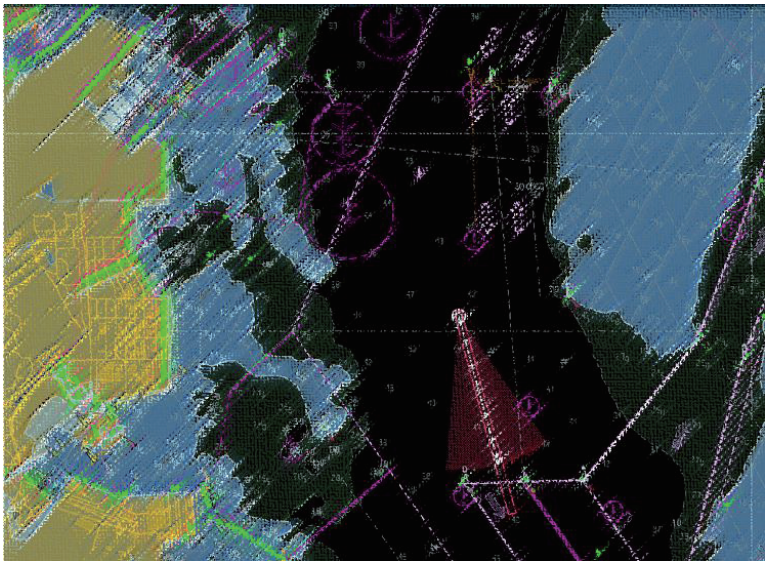
JAPAN P&I CLUB



ECDISのGPSの位置データは正確？

航海士は、次の重要性に留意する必要があります。

- GPS は、妨害電波等のため正確な位置を表示しないことがあること。
- 目視によるクロストラック(XT)、及びレーダーとのレーダーオーバーレイによる定期な本船位置の確認。
- 会社の航海当直手順の再確認。

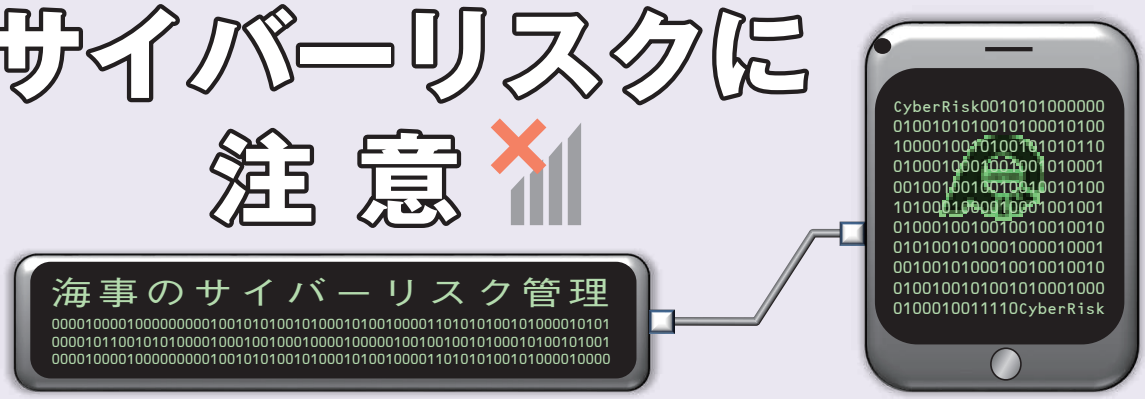


ICS Bridge Procedure Guide によれば、
ECDIS は安全な航海のための支援装置。つまり、ECDIS 自体は安全な航行を行っているわけではなく、
安全航行という船長や当直航海士の責務を緩和するに過ぎません。

船橋掲示

JAPAN P&I CLUB

サイバーリスクに注意



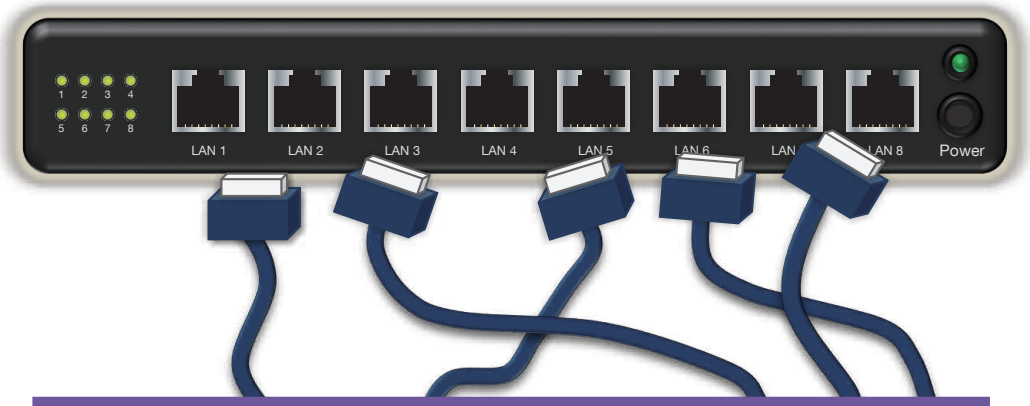
乗組員は、システムの統合者ではないよね？

船主の許可なく、乗組員によりLANケーブルを交換した結果、
船内のコンピュータベースのシステムが**誤動作**を引き起こした。

IACS UR E22（Rev.1） は、監視システムといった機械システムに使用されるコンピュータベースのシステムの構成および機能に関連する要件を規定する。

3.3.2. 変更管理

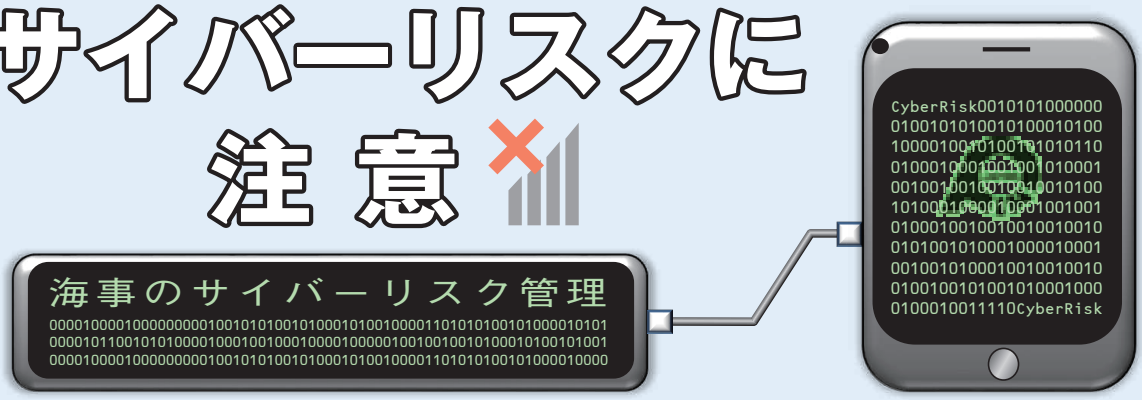
船舶所有者は、ソフトウェアおよびハードウェアの変更管理に必要な手順書が船上に存在し、また、ソフトウェアの変更/更新がその手順書に従って実施されていることを保証する必要がある。運用段階におけるコンピュータベースのシステムに対するすべての変更履歴は、記録し、履歴を確認できるようにする。



**全ての乗組員及び訪船者は、
本船のシステムのセキュリティ手順に厳密に従うこと。**

JAPAN P&I CLUB

サイバーリスクに注意



本船のPCに対してスキャンを使用して、制限を設けていますか？

U ウイルス対策ソフトウェアの定期的な更新同様、承認された者のみが使用する。

S 使用するときはいつでも、スキャン機能を使用する。

B 港内では本船PCに対して立ち入り制限を設け、USBの使用にはそのリスクを検討する。

- **USB メモリー接続によって、業務 PC にウイルス感染することが一般的なウイルス感染の根本原因となっている。**
- **乗組員全員がリスクに十分に留意しなくてはならない。**

公共スペース、船橋、士官室および機関制御室掲示

JAPAN P&I CLUB

著者近影

日本船主責任相互保険組合
ロスプリベンション推進部
マネージャー　日野岳彦

JAPAN P&I CLUB
日本船主責任相互保険組合
ウェブサイト http://www.piclub.or.jp

●東京本部　〒 103-0013　東京都中央区日本橋人形町 2 丁目 15 番 14 号 …… Tel：03-3662-7229　Fax：03-3662-7107
●神戸支部　〒 650-0024　兵庫県神戸市中央区海岸通 5 番地 商船三井ビル 6 階…… Tel：078-321-6886　Fax：078-332-6519
●福岡支部　〒 812-0027　福岡県福岡市博多区下川端町 1 番 1 号 明治通りビジネスセンター 6 階　… Tel：092-272-1215　Fax：092-281-3317
●今治支部　〒 794-0028　愛媛県今治市北宝来町 2 丁目 2 番地 1 …… Tel：0898-33-1117　Fax：0898-33-1251
●シンガポール支部　80 Robinson Road #14-01 SINGAPORE 068898 …… Tel：65-6224-6451　Fax：65-6224-1476
Singapore Branch
● JPI 英国サービス株式会社 5th Floor, 38 Lombard Street, London EC3V 9BS U.K. …… Tel：44-20-7929-3633　Fax：44-20-7929-7557
Japan P&I Club（UK）Services Ltd