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

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

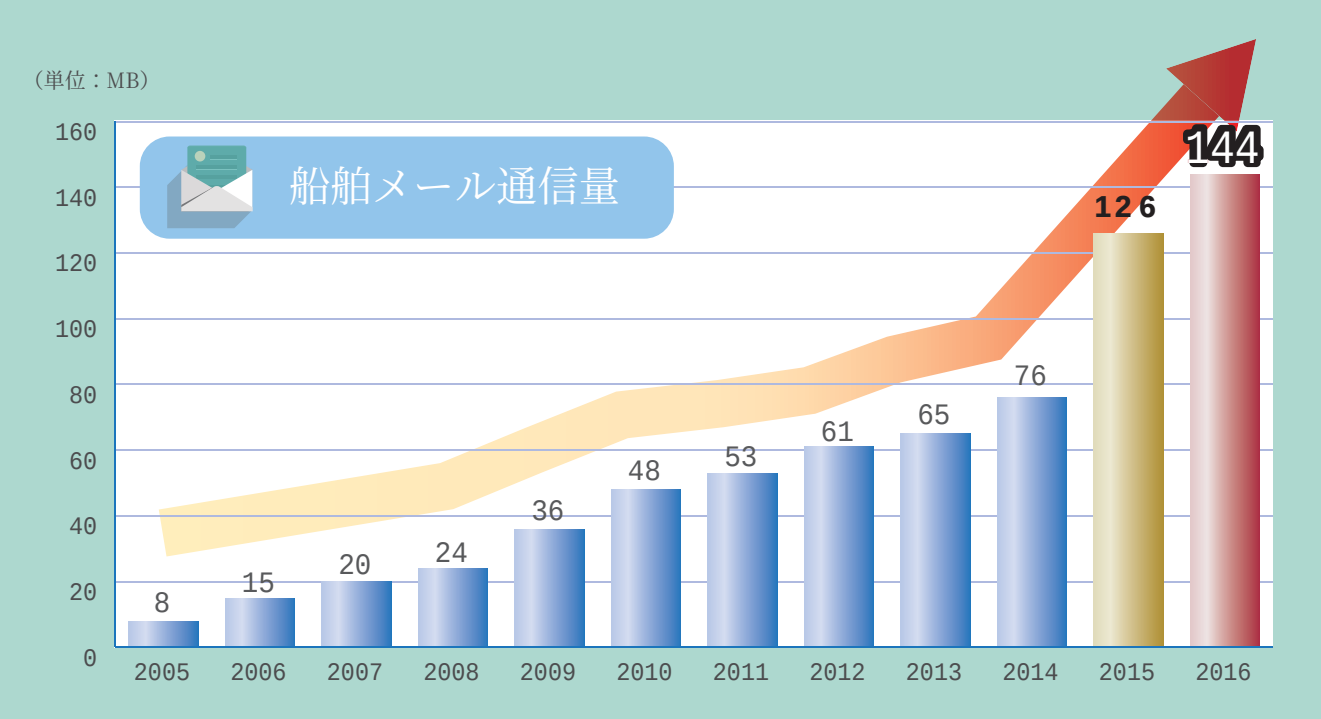
当組合の保険契約規定ではサイバーリスクを特定した規定はありませんが、もしサイバー攻撃や侵害によるクレームが起きた場合は現行の保険契約規定に則り通常通りにてん補の可否を検討します。サイバー攻撃が保険契約規定の第 35 条の「戦争」や「テロ行為」に該当しないと判断された場合、通常の P&I 保険によるてん補の対象となりえます。
例えば、乗組員の個人 PC、本船業務用の E-mail PC を経由して船内 LAN システムにウイルスが感染してしまった、または本船で業務 PC を許可なく Update してしまった、または本船で乗組員が許可なく船内 LAN ケーブルを繋ぎ変えた結果、航海用電子器機器や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

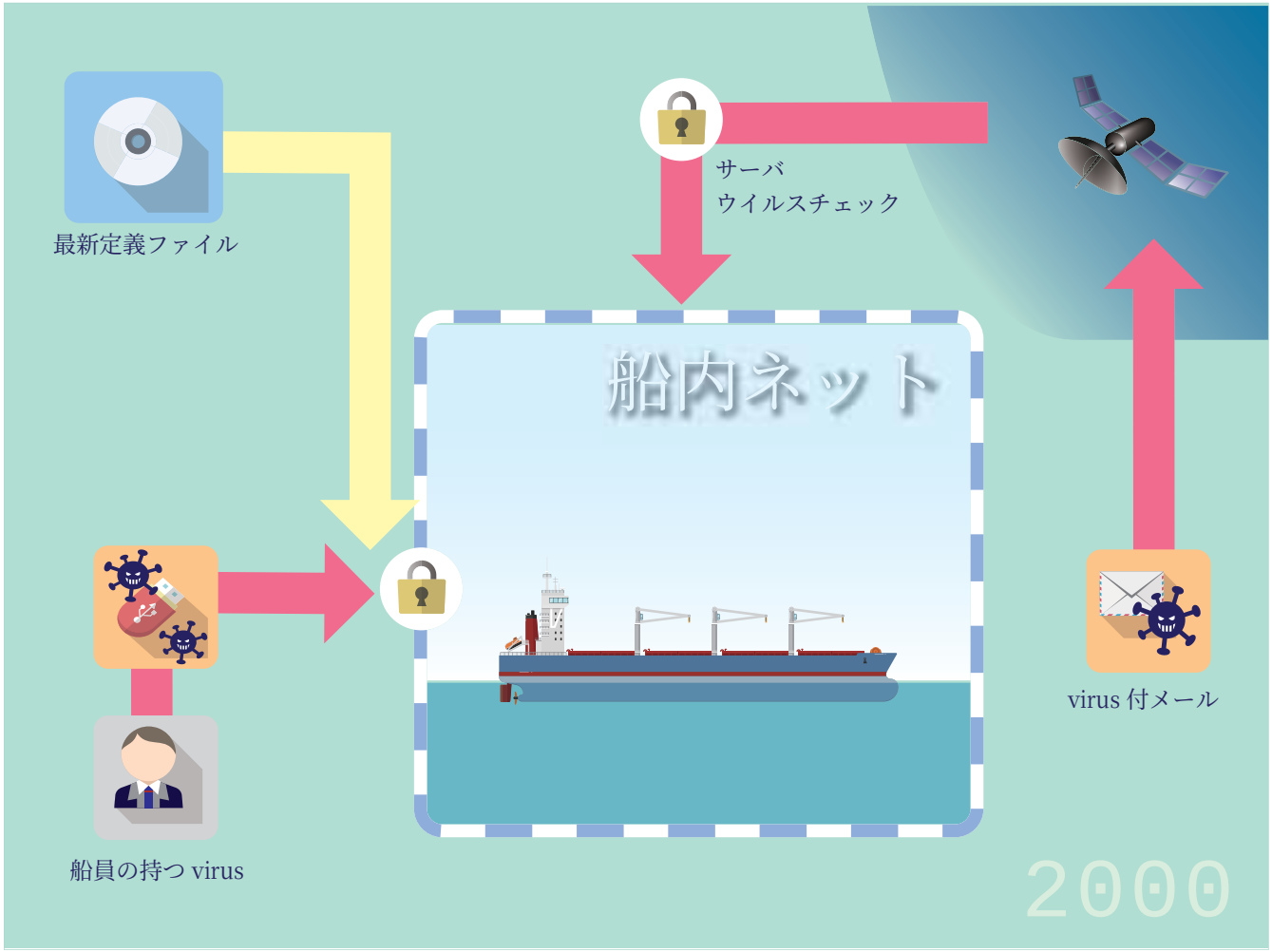


図 2. 2000 年頃

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。

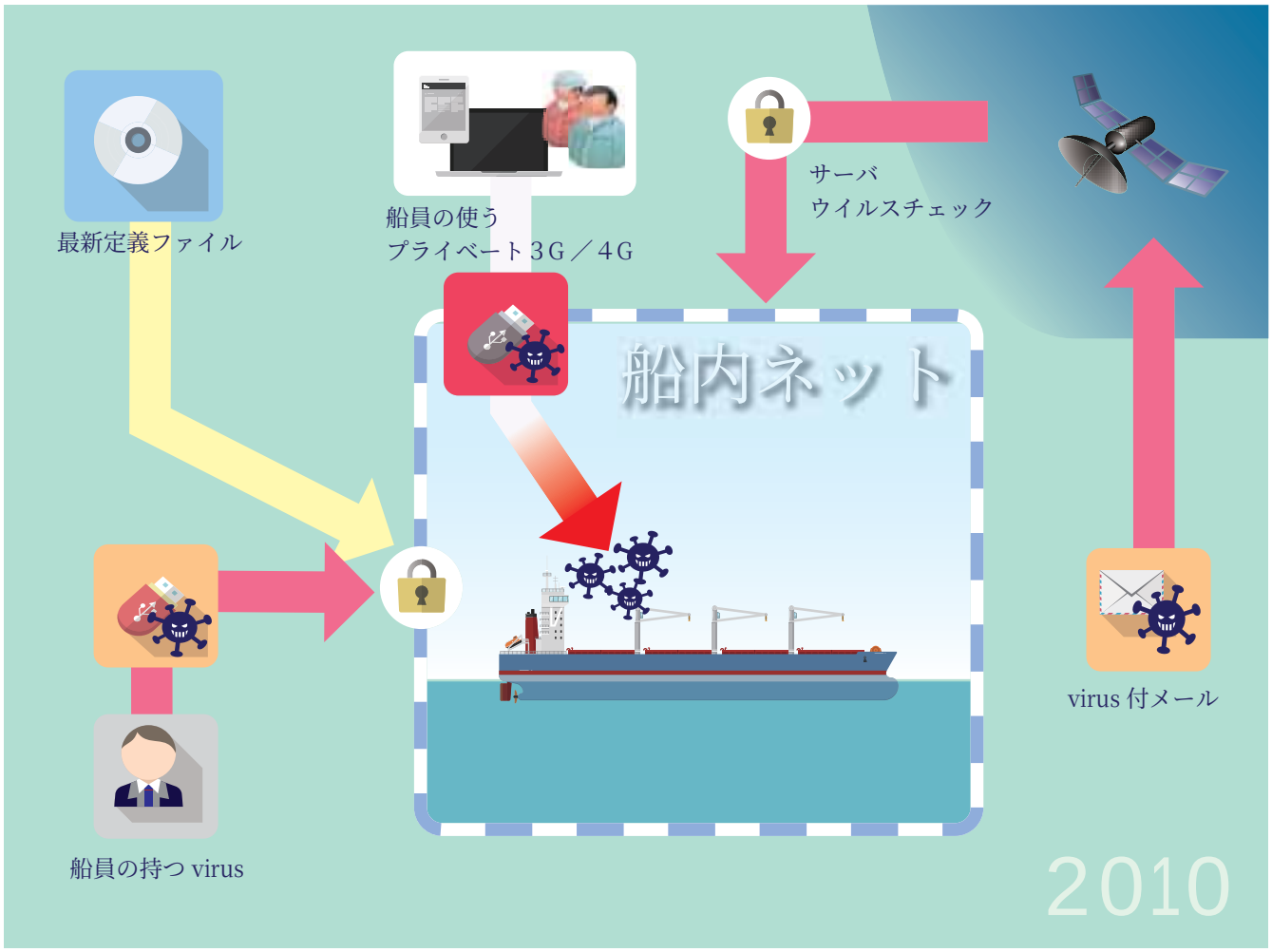


図 3. 2010 年頃

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。

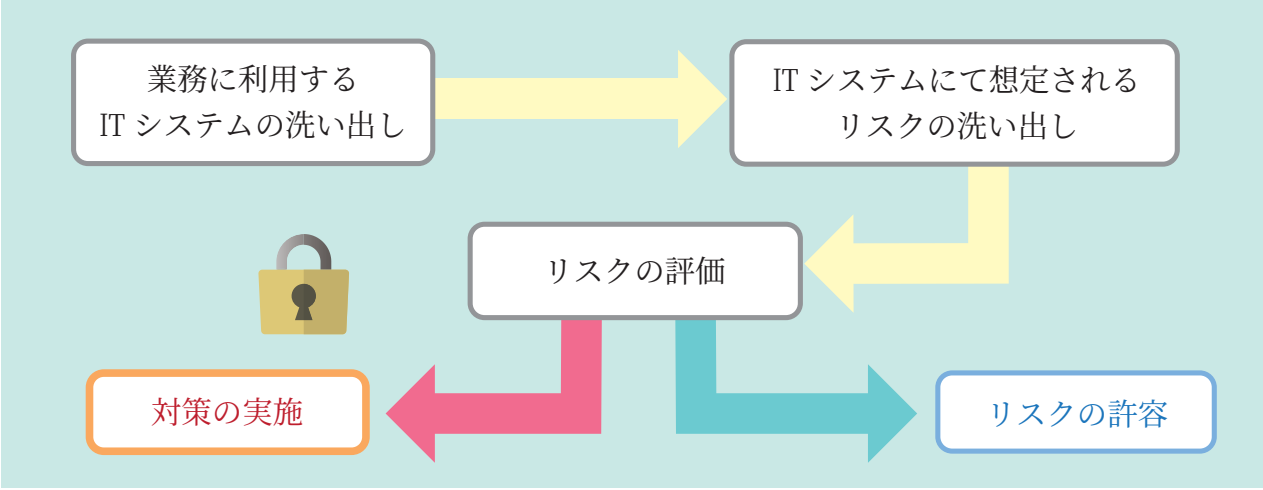
本ガイド後半では、船舶 IT 分野で実績のある株式会社オルカが、サイバーセキュリティ対策のリスクアセスメントのアプローチ手法を用いて MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management を想定した SMS の雛型を紹介しています。

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）

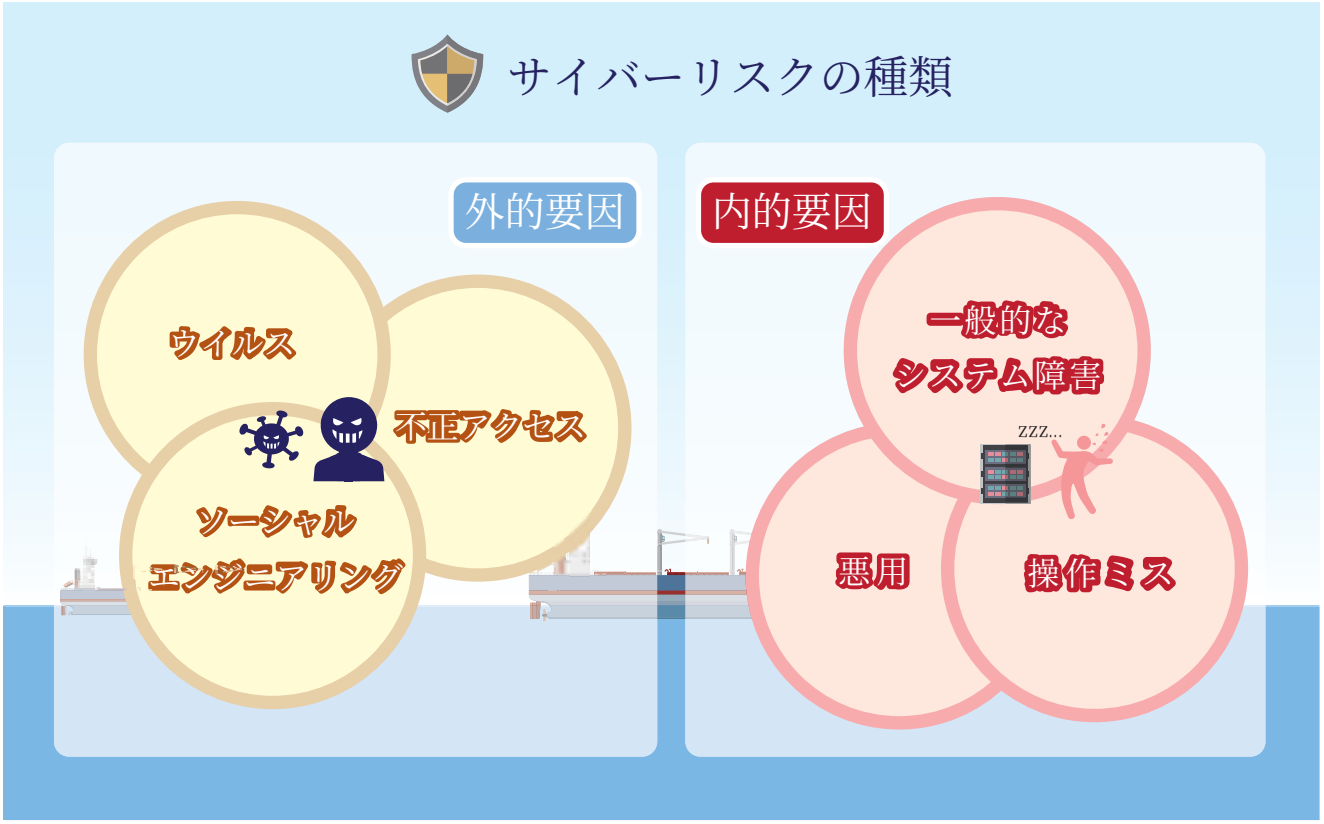
各コンピュータシステムのサイバーセキュリティ対策の責任の所在は各コンピュータシステムの供給者（Supplier）と定義されておりますが、システムを接続した場合は単体での運用では想定されないリスクが新たに発生するため、システムの統合者（System integrator）に責任が求められることになります。

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

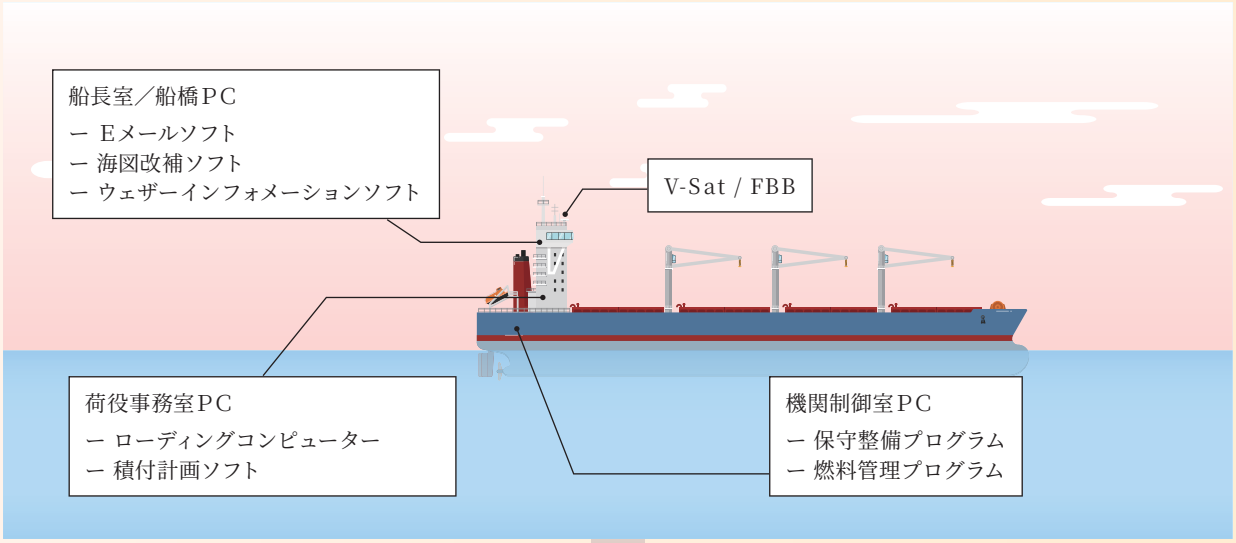
サイバーリスクというとシステムの不正アクセスやハッキングなど、外的要因が注目されがちですが、操作ミスや一般的なシステム障害といった内的要因も存在しているということを再度見つめなおす必要があります。



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

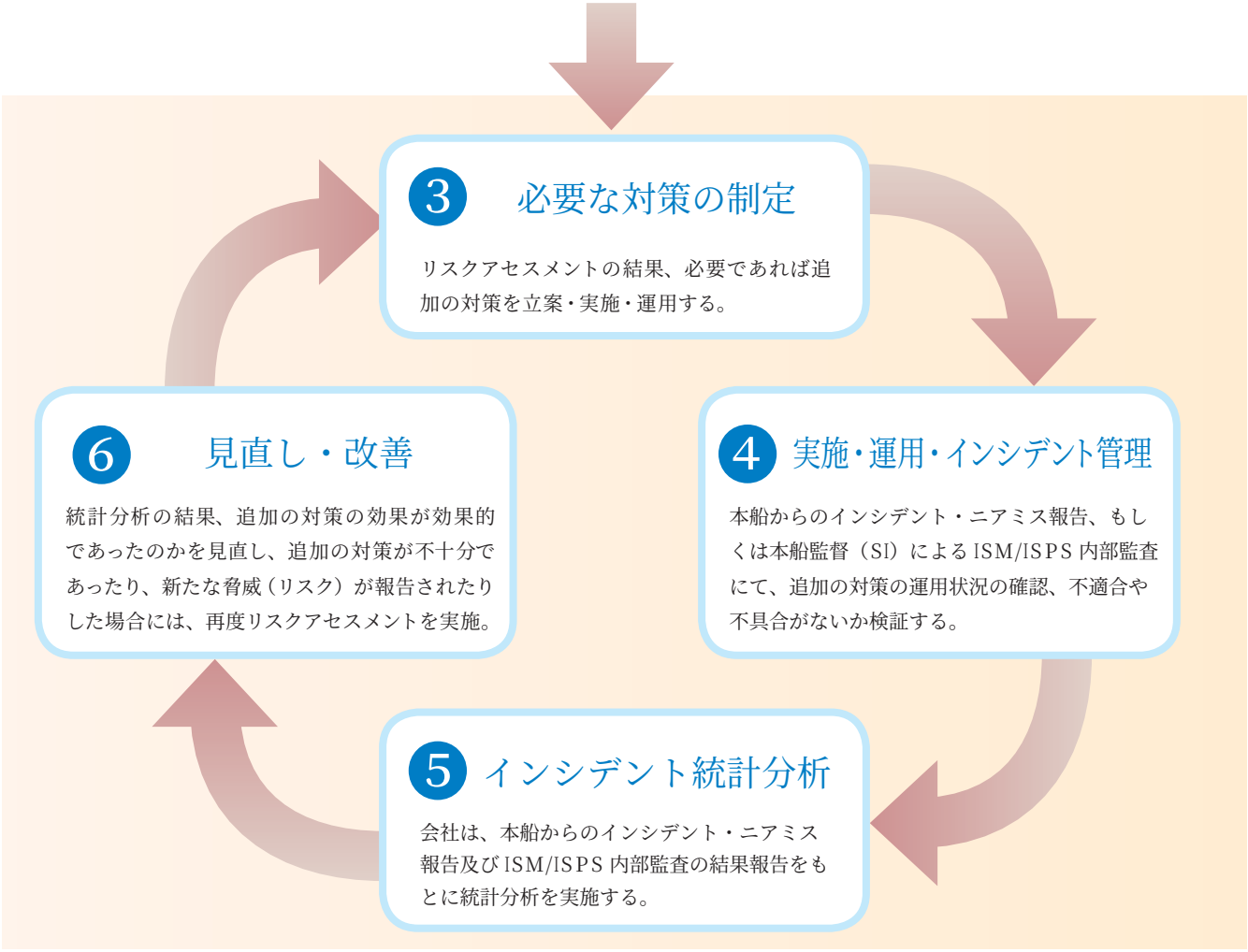
リストアップした IT システム毎に対して、起こる結果（損害）と頻度、既存の管理手法を検討しながらリスクアセスメントを実施する。

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。

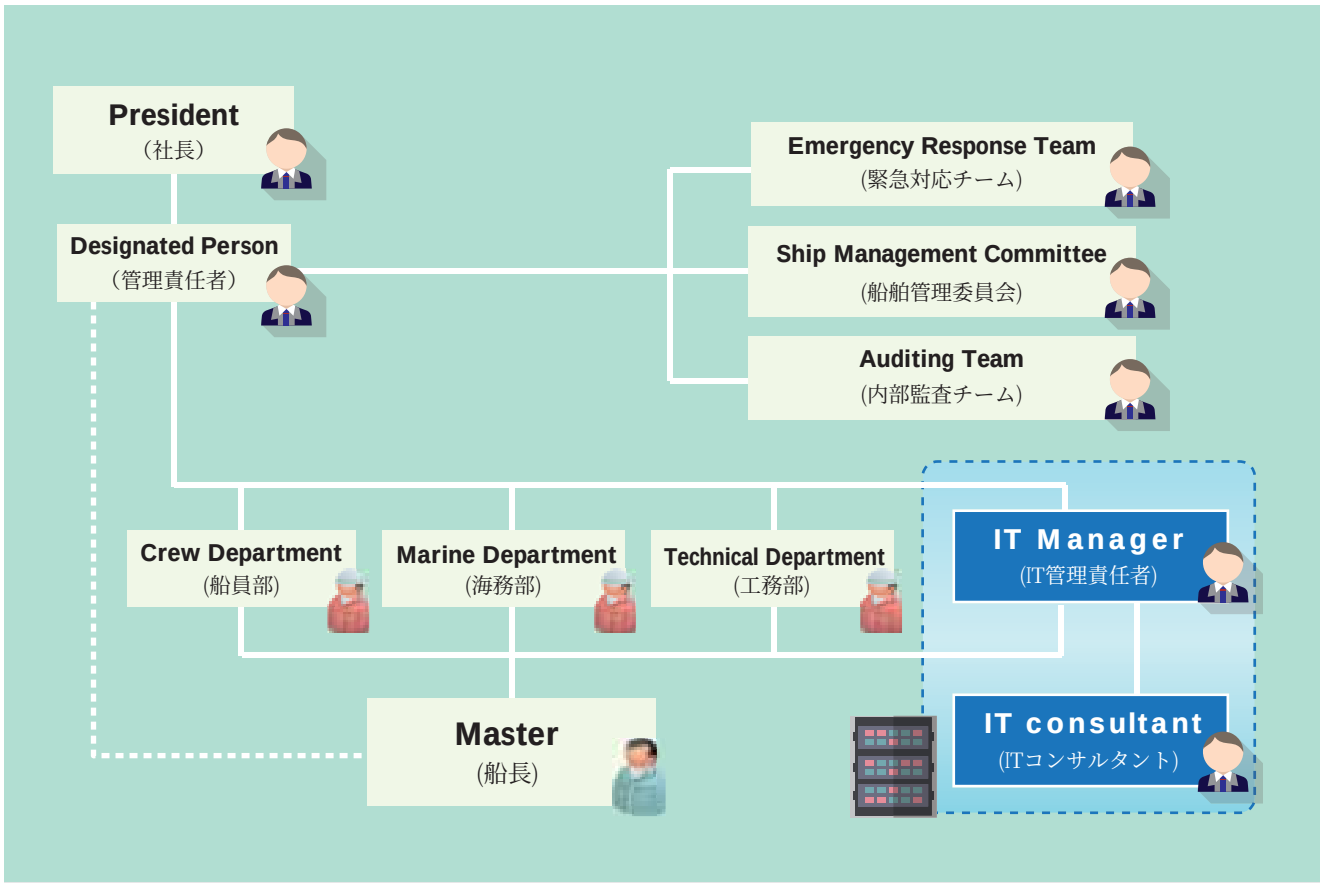
❹…… 本船からのインシデント・ニアミス報告もしくは、本船監督（SI）によるISM内部監査にて、追加の対策の運用状況の確認、不適合や不具合がないか検証する。

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。

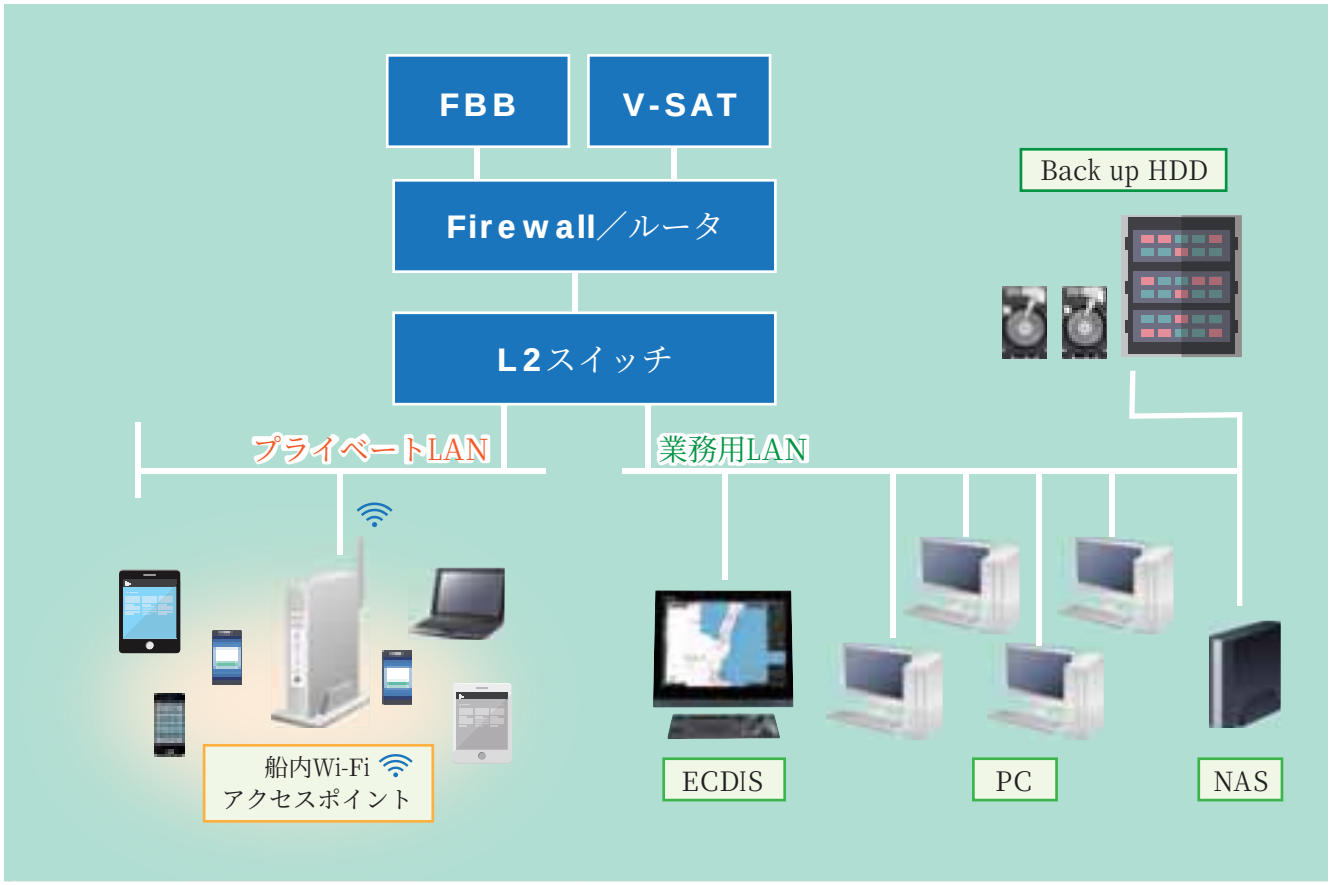


図 5. 船内 LAN の構築例

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」