JAPAN P&I CLUB　第48号 2020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

## 補 足 版

# 目　次



# はじめに

2020 年はじめに、日本を代表する防衛関連企業 4 社への大規模なサイバー攻撃が明るみに出ました。海事分野におけるサイバーセキュリティの関心は、特定海域での GPS 乗っ取り（Spoofing）問題等もあり、急速に高まっています。そして外航船を運航される船会社におかれましては翌年 2021 年以降初回の会社審査（DOC：Document of Compliance）までにサイバーセキュリティマネージメントを SMS へ取り込むように IMO ガイドラインで推奨されています。この IMO ガイドラインは強制ではないものの、各旗国は同ガイドラインに則り対応するよう求めています。本ガイドは、2018 年 5 月に発行したロスプリベンションガイド 42 号「サイバーリスクとサイバーセキュリティ対策」の補足版として、船舶運航上でのトラブル事例や外部監査の指摘などを紹介し、サイバーセキュリティマネージメントの立案や、既に運用中のセキュリティマネージメントの見直しに役立てて頂ければと思います。

# IMO サーキュラー

### 2014 年 11 月 - 第 94 回海上安全委員会（MSC 94）

海事分野のデジタル化によりサイバーシステムへの依存が劇的に増加していることを踏まえ、船舶、港湾、海洋設備の保護とサイバーシステム支援のレジリエンス向上のため、サイバーセキュリティガイドラインの策定について提案されました。

### 2016 年 5 月 – 第 96 回海上安全委員会（MSC 96）

第 96 回海上安全委員会（MSC 96）では、業界ガイドライン及び国際規格を盛り込んだ非強制のサイバーセキュリティ対策に関する暫定ガイドライン MSC.1/Circ.1526 が承認されました。同ガイドラインは、個々の機器やシステムに着目した詳細な要件を規定するものではなく、サイバーリスク管理のために考慮すべき要素が示されました。

### 2017 年 6 月 – 第 96 回海上安全委員会（MSC 98）MSC.428（98）

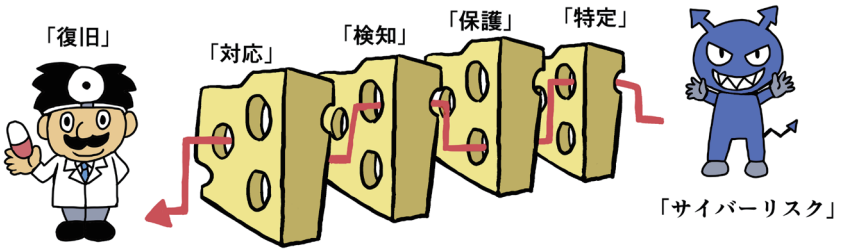
MSC 決議（MSC.428（98）：Maritime cyber risk management in safety management systems）が採択され、ISM コードに基づく安全管理システムを通じてサイバーリスク管理を実施することが推奨されました。
海事サイバーリスクマネジメントのガイドラインは MSC.1/Circ.1526 として承認されていたものを改めて、MSC 及び FAL の合同回章（MSC-FAL.1/Circ.3：Guidelines on maritime cyber risk management）として承認されました。

**IMO ガイドラインでは、**

**効果的なサイバーリスクマネジメント策定のために**

**以下の要素を定めています。**

- 「特定」個人の役割及び責任を明確にして、妨害を受けたときに船の運航にリスクをもらすシステム、財産、データ、性能を特定しておくこと。
- 「保護」リスク制御のプロセス及び対策、並びにサイバーイベントから保護するためのリスク軽減計画を実施して、継続的な運航を確保すること
- 「検知」サイバーインシデントをタイムリーに検知するために必要な行動を検討しておくこと。
- 「対応」レジリエンスを備え、船舶運航に必要なシステムやサイバーインシデントにより妨害されたサービスを復元するための行動計画を検討しておくこと。
- 「復旧」サイバーインシデントの影響を受けた、船舶運航に必要なシステムをバックアップし、復旧するための対策を準備すること。




# 旗国サーキュラー
# 船級協会

## 旗国サーキュラー

パナマ
Maritime Cyber Risk Management
-MERCHANT MARINE CIRCULAR MMC-354

マーシャル諸島
Maritime Cyber Risk Management
-Maritime Cyber Risk Management No. 2-11-16

リベリア
Maritime Cyber Risk Management
-MARINE SECURITY ADVISORY – 02/2019

上記のように、主要な旗国は IMO ガイドラインに則り SMS（ISPS を含む）にサイバーセキュリティマネージメントを取り入れるよう求めています。
＊最新情報は常に各旗国及び船級と、ご確認をお願いいたします。

## 船級協会

一般財団法人日本海事協会（ClassNK）では、以下を 2019 年に発行しています。
「サイバーセキュリティシリーズ」として、
① 新造船設計に関わる「船舶におけるサイバーセキュリティデザインガイドライン」
② 船舶管理を対象とした「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」
③ 舶用ソフトウェアを対象とした「ソフトウェアセキュリティガイドライン」
そして ClassNK の関連会社である株式会社 ClassNK コンサルティングサービスが、BIMCO（ボルチック国際海運協議会）ガイドライン Ver3.0 に適合した e-learning 方式のサイバーセキュリティ教育コンテンツの提供（日本語、英語対応）を 2020 年 3 月に開始しています。

# BIMCO サイバーセキュリティ条項
## （BIMCO Cyber Security Clause）2019

2019 年に公表された BIMCO サイバーセキュリティ条項では、危険の認識、サイバーインシデント発生時に対応するためのシステムの導入、サイバーリスク発生時に影響を最小化する義務を定めています（条項全文は巻末に掲載しています）。

（a）項では、当事者双方による「適切な」サイバーセキュリティ施策とシステムを導入及び維持することを要請しています。

（b）項では船主・傭船者を代理して業務を行う第三者（例えば、デジタルでサービスや情報を提供するブローカーや代理店等）に適切なサイバーセキュリティを導入するよう合理的な努力をすることを要請しています。

（c）項ではサイバーインシデントを検知した場合の対応について規定しています。実務上可能な限り早く、最初の通知を受領してから 12 時間以内に、代替的連絡先と、サイバーインシデントによる影響を最小化・防止しうる情報を提供することが求められます。

（d）項では本条の義務違反による責任について、責任限度を設けることと、当該責任限度額を定めています。ブランクフォームは限度額の欄は空欄でありますが、空欄のままにすると USD100,000 で合意したこととなります。
ただし、責任を負うべき当事者の一方的な故意または重過失に基づく場合は、当該上限を適用しないこととしています。

**小川総合法律事務所「第 39 回海事契約ワークショップ」より要約**

日々巧妙化するサイバーリスクに対し、サイバーセキュリティマネジメントを考えていくには、運航船が被害に遭うことを前提としておかなければなりません。そして、サイバーインシデントが発生した時、あるいは、検知した際には、その状況を遅滞なく IT 管理者やその他関係者へ連絡して対処方法の指示を仰ぐことが重要です。そのための第一歩は本船と本船関係者からの報告です。

# 事例紹介

## 事例 1

**新たに導入した船主（会社）側の Anti-Spam サーバに用船社のメールがひっかかってしまった。**


**原因**　迷惑メールを誤検出、ネットワーク管理者不在

## 事例 2

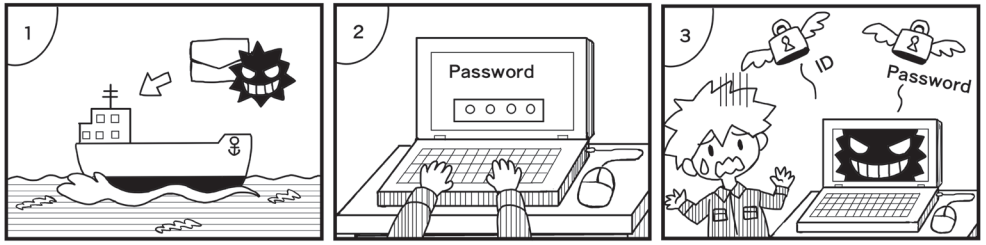
**導入した Anti-Virus のメールスキャンが船舶メール送受信に影響を与えた。**

**原因**　十分な検証なしに陸上と同じ Anti-Virus を本船 PC に導入

## 事例 3

**本船船長が Phishing Mail にひっかかってパスワードが漏れてしまった。**

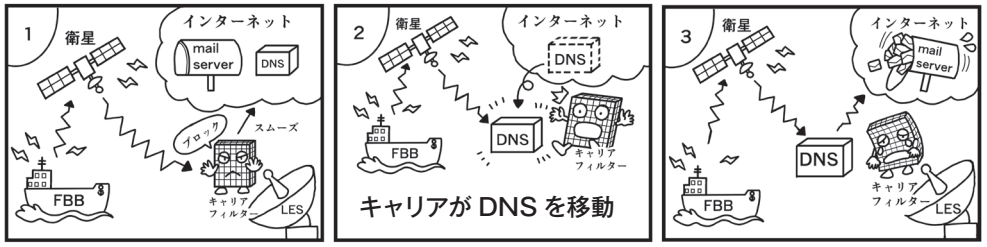
**原因**　本船 PC の IE・OS の未更新、本船船長の IT リテラシーの欠如




## 事例 4

**通信費が突然増加（突然、毎月の通信量が 100MB 増加）してしまった。**

**原因**　通信キャリアが DNS サーバの位置をユーザーに連絡なく移動




## 事例 5

**船内 LAN が停止してしまった。**

**原因**　業者により船内監視カメラシステムの LAN と通信用 LAN を誤って接続

## 事例 6

**船内 LAN が停止してしまった。**

**原因**　船員が勝手に施設したプライベート用 WiFi – AP（アクセスポイント）を設置し、業務用 LAN にまで影響が発生


## 事例 7

**船内 LAN 通信不安定**

**原因**　造船所が敷設した LAN ケーブルの圧着不良が原因で、就航後の振動等により物理的に LAN 接続が不安定となった

## 事例 8

**電子海図更新ソフトのバージョンアップを実施後に、通信不能となった。**

**原因**　バージョンアップに伴い、通信に必要なポート番号が変更されており、担当 SI から通知がなかったためにシステム管理者はその事実を把握していなかった

## 事例 9

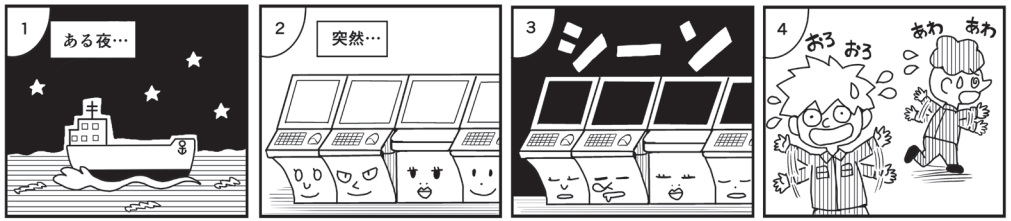
**VSAT 導入後、速度制限を受けメール通信が不調となってしまった。**

**原因**　VSAT の通信キャリアの固定費用プラン（Unlimited plan）を採用したが Committed Information Rate（最低速度保証）がないプランであったため、速度制限を受けた状況下で必要な通信が正常に動作しなかった

## 事例10

**中国のある港に向けて夜間航行中に、ECDIS4 台とレーダー 3 台が同時にシャットダウンしてしまった。**

**原因**　後日、陸上の技術者が調査したところ ECIDS やレーダーのシステム統合上のシステム設定（ECDIS 同士の Primary と Secondary の設定を含む）の問題であったことが判明




# 外部監査等での指摘事例

以下のような外部検査や監査での指摘事例については、IT 管理責任者からアドバイスやリスクアセスメント結果をフィードバックしてもらい、実行の必要性を検討してください。

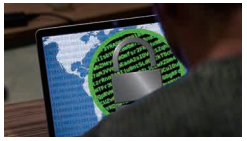
① サイバーセキュリティ緊急対応計画（Cyber Security Response Plan）が手順書にない。

② PC や機器に USB ポートカバー、LAN ポートカバーがない。

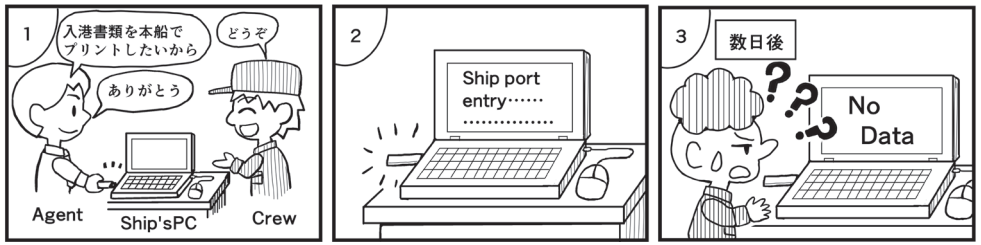
③ OS をアップデートしていない （保守サービスが終了した version の使用）。

④ 訓練という意味でのフィッシングテスト（Phishing test）を実施していない。

⑤ いわゆる第３者によるハッキングテスト（Penetration test）を実施していない



# 実際に本船運航の現場では




船内ネットワークや船内 PC にウィルス感染してしまうような可能性のある場面は以下のような場合などが考えられます。

- 船用機器整備や修理業者から彼らのサービスレポートを本船 PC 及びプリンターで印刷するように頼まれる場合
- 船員が本船のデータ（写真やファイル）を使用する、あるいはデータ保存するため本船の共有 PC に、個人 USB を利用する場合
- 船員個人のスマートフォンから業務用 WiFi にアクセスする場合　　など

このようなコンピューターウィルスの感染防止対策として、本船に安全にデータを受け渡しできるような機器を本船に備えていたり、またこのような状況に対応する会社手順があり、船員向けに指導・教育を実施していますか？また、船舶管理会社の監督（SI）も IT や最新のソフトウェアや ECDIS に対して十分な知識を持っておらず、船舶検査や監査の場面で十分な確認が出来ていないということはないですか？


本ガイドで紹介した事例は、サイバーセキュリティマネージメントによる適切な管理・運用や教育が、会社と船員と双方で実施されていなかったことが根本原因と推測されるものが大半を占めております。
一方、船員の SNS（ソーシャル・ネットワーキング・サービス）に関わるトラブルとして、秘匿性の高い貨物情報の拡散、会社の許可なく事故情報 / 事故画像を拡散してしまう、船内での不安全行動を公開する、関係者の個人情報の暴露といった船員個人レベルにおけるセキュリティマネージメントも注目されています。
また、船員同士で Crew 用 WiFi のデータ容量を売買するといった新たな船内不和につながりうる事象も出てきております。

サイバーセキュリティマネージメントを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前回のロスプリベンションガイド 42 号でも触れました。そして 2019 年春季に当組合で実施したアンケートでは、「IT ポリシーを準備していない」、「IT 管理責任者を選任していない」、「船員の SNS、ブログ利用に関してルールを設けていない」という回答が、約 6 割ありました。
事故等の緊急対応や定期訪船での本船システム保守や、新システム導入に際して、IT 管理責任者の役割と責任は重要です。もし社内に適任者がいない場合には、社外の専門家に、相談できる体制を確立しておくことも一つの対応策と考えます。

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。

**参考文献**


- MSC.1/Circ.1526
- The Guidelines On Cyber Security Onboard Ships ver3
- Maritime Cyber Risk Management　-MERCHANT MARINE CIRCULAR MMC-354
- Maritime Cyber Risk Management　-Maritime Cyber Risk Management No. 2-11-16
- Maritime Cyber Risk Management　-MARINE SECURITY ADVISORY – 02/2019


**添付**

- BIMCO サイバーセキュリティ条項（BIMCO Cyber Security Clause 2019）
- 当組合試訳　分野：No.28 サイバーセキュリティ（Dry Bulk Management Standard）
- サイバーセキュリティマネージメントポスター

## BIMCO Cyber Security Clause 2019

In this Clause the following terms shall mean:

"Cyber Security Incident" is the loss or unauthorised destruction, alteration, disclosure of, access to, or control of a Digital Environment.

"Cyber Security" is technologies, processes, procedures and controls that are designed to protect Digital Environments from Cyber Security Incidents.

"Digital Environment" is information technology systems, operational technology systems, networks, internet-enabled applications or devices and the data contained within such systems.

(a) Each Party shall:

(i) implement appropriate Cyber Security measures and systems and otherwise use reasonable endeavours to maintain its Cyber Security;

(ii) have in place appropriate plans and procedures to allow it to respond efficiently and effectively to a Cyber Security Incident; and

(iii) regularly review its Cyber Security arrangements to verify its application in practice and maintain and keep records evidencing the same.

(b) Each Party shall use reasonable endeavours to ensure that any third party providing services on its behalf in connection with this Contract complies with the terms of subclause (a)(i)-(iii).

(c) If a Party becomes aware of a Cyber Security Incident which affects or is likely to affect either Party's Cyber Security, it shall promptly notify the other Party.

(i) If the Cyber Security Incident is within the Digital Environment of one of the Parties, that Party shall:

(1) promptly take all steps reasonably necessary to mitigate and/or resolve the Cyber Security Incident; and

(2) as soon as reasonably practicable, but no later than 12 hours after the original notification, provide the other Party with details of how it may be contacted and any information it may have which may assist the other Party in mitigating and/or preventing any effects of the Cyber Security Incident.

(ii) Each Party shall share with the other Party any information that subsequently becomes available to it which may assist the other Party in mitigating and/or preventing any effects of the Cyber Security Incident.

(d) Each Party's liability for a breach or series of breaches of this Clause shall never exceed a total of USD _____ (or if left blank, USD 100,000), unless same is proved to have resulted solely from the gross negligence or wilful misconduct of such Party.





## 当組合試訳

### 分野：No.28 サイバーセキュリティ（Dry Bulk Management Standard）

2020 年 4 月、安全へのサポートツールとして Dry Bulk Management Standard（DBMS）が、リリースしました。この基準はまだドラフト段階でありますが、ドライバルクの業界のベンチマークとなるような 4 段階（初級、中級、上級、優秀）の指標が示されています。
サイバーセキュリティ対策立案の参考として活用できるものと考えます。

分野：No.28 サイバーセキュリティ

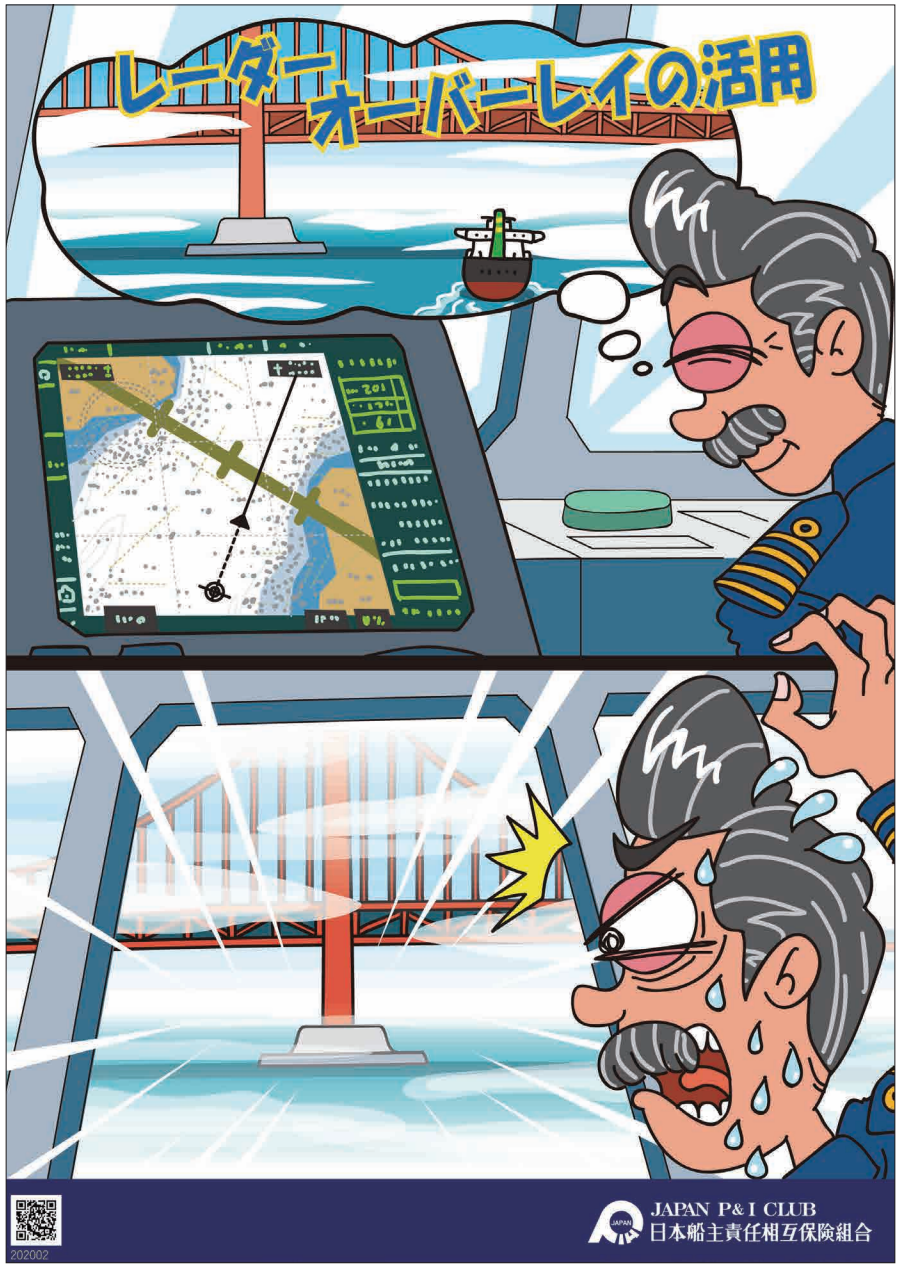
**基本方針**：
会社は情報の完全性・可用性・機密性とシステムのためのリスク管理するための IT およびデジタルプロセス制御システムを設計と運用するプログラムを持つ。

| レベル | 期待 | ターゲット | 客観的証拠 |
|---|---|---|---|
| 初級 | 会社は、サイバーセキュリティに対応した文章化されたポリシーと手順を持っている。<br><br>会社は、サイバーセキュリティ評価を実施し、サイバーセキュリティ計画を策定している。<br><br>会社は、サイバーインシデントに対応し、サイバーインシデントから復旧する手順を用意している。<br><br>会社は、サイバーセキュリティの責任者を陸上及び本船上に適切に選任している。 | シニアマネージメントによって署名されたポリシーには、サイバーインシデントの影響を最小限に抑えることへのコミットメントが含まれている。<br><br>評価には、外部及び内部のサイバーセキュリティ上の脅威、通信リンクと本船上の IT と OT の識別、これらのシステムに対するサイバーセキュリティ上の脅威の影響の識別が含まれる。<br><br>計画には、脆弱性が悪用される頻度を下げ、脆弱性が悪用されることによる潜在的な影響を下げる対策が含まれる。 | ポリシーと手順<br><br>サイバーセキュリティ評価<br><br>サイバーセキュリティ計画<br><br>サイバーインシデントからの復旧手順<br><br>陸上及び本船上の責任者の任命<br><br>訓練と能力 |

| レベル | 期待 | ターゲット | 客観的証拠 |
|---|---|---|---|
| **中級** | 会社は、本船上の IT/OT システムへの物理的なアクセス制御と個人用デバイスの使用に関する手順を文書化している。 | 手順には、重要機器の攻撃からの保護、USB ポートを含む通信ポートへのアクセスコントロール、個人用デバイスの使用や第 3 者のアクセス、サーバーを含む全ての IT/OT 端末へのアクセスコントロールがといったものがある。 | KPI 指標の手順化 |
| | 会社はすべての職員にサイバーセキュリティ訓練を提供している。 | 全ての陸上と本船乗組員は、サイバーセキュリティポリシーとその要件、そしてサイバーセキュリティにどのように貢献するのか、またそのポリシーに準拠しない場合の影響を認識しておく必要がある。初回および復習のトレーニングが提供される。 | 全職員の訓練と記録の保持 |
| | 会社は、サイバーセキュリティ手順の内部監査を実施し、その有効性を検証している。 | サイバーの内部監査は手順書化されており、会社は監査計画を作成している。 | サイバーセキュリティ監査 |
| | 会社は、潜在的なサイバーセキュリティイベントに対応するため、情報を常に受信出来るように情報源を形式化している。 | | |

| レベル | 期待 | ターゲット | 客観的証拠 |
|---|---|---|---|
| **上級** | 会社は、その適切性、妥当性および有効性を確保するためにサイバーセキュリティ計画の効果を検証する。 | 計画の実行と発展をフォローアップするために少なくとも年に一回はマネジメントレビューを実施する。 | マネージメントレビューの文書化 |
| | 会社は、第 3 者のアクセス管理を実施している。 | 会社は、第 3 者による IT および OT へのアクセスに適切な予防策を実施している。 | 第3者アクセスの予防策デューデリジェンス監査 |
| | | 会社は、システムへのアクセス許可前に、デューデリジェンス監査を実施するか、独立監査人のレポートを使用する。 | |
| | | 本船と本船の機器はサイバー脆弱性を抑えるようにデザイン設計されている。会社は、フリートに新しいテクノロジーを採用する前に、決められたプロセス手順を持っている。 | 新しい機器のためのサイバーセキュリティ評価 |
| **優秀** | 会社は、外部リソースを利用して定期的な監査を実施し、サイバーセキュリティ計画の順守を確認する。 | 監査は、会社が遵守しなければならない外部制度のコンプライアンスを理解し、サイバーセキュリティ手順の内部的コンプライアンスの確認、サイバーリスク評価とリスク状態を確認することに利用される。 | サイバーセキュリティ計画の外部監査 |
| | 会社は、すべてのフリート船舶でサイバーセキュリティ符号の取得をしている。 | 会社は ISO270324 を取得および、または船舶の船級符号を取得している。 | 証書 |
| | 会社は、ネットワーク侵入監視およびその他の高度なサイバーセキュリティ監視サービスを取り入れて、重要なシステムを保護するための多層防御をしている。 | 会社は、重要なシステムのネットワーク攻撃への暴露を制限し、ネットワークトラフィックを監視し、侵入を試みたあるいは実際のネットワーク侵入を検出して対応するテクノロジーを使用している。 | サイバーセキュリティ監視サービスの使用 |

サイバーセキュリティマネージメントポスター




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
コーポレートサイト　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　今治北宝来町ビル 5 階
Tel：0898-33-1117 Fax：0898-33-1251

●シンガポール支部　Singapore Branch
80 Robinson Road #14-01 SINGAPORE 068898
Tel：65-6224-6451 Fax：65-6224-1476

● JPI 英国サービス株式会社　Japan P&I Club（UK）Services Ltd
5th Floor, 38 Lombard Street, London EC3V 9BS U.K.
Tel：44-20-7929-3633 Fax：44-20-7929-7557