船舶サイバーセキュリティ対策で求められること

―ある船舶が座礁しました。サイバーインシデントではないと言い切れますか？―

マリンネット㈱代表取締役社長　**谷繁　強志**

あなたが操船している若しくは管理している船舶が、予定航路を外れ、座礁をしました。原因は定かではありませんが、サイバーリスク・サイバーセキュリティの観点からも、検証されるべきです。サイバーインシデントがあったのかどうか、なかった場合にどのようなレポートを提出するのか。船舶のサイバーセキュリティ対策とは、サイバーアタックを防ぐばかりではなく、サイバー上何があったのか検証できることも含むものと考えられます。

船上において、若しくは陸上において、船舶におけるサイバーセキュリティに関し対策をしなければいけない機運が高まっています。米国でも強制化が発表されました。でも、何から手をつけて良いのかわからない、取組み始めているが、手法は合っているのか不安という方も多いのではないでしょうか？中々明確な回答が未だ無く、我々も日々ClassNKをはじめ様々な人たちと意見交換をしながら、船舶サイバーセキュリティ対策を推進しています。

＜マリンネット会社紹介＞

マリンネットは、マリンネットサイトで業界ではおなじみですが、2000年のITブームの時に設立されたITカンパニーです。船舶管理会社さん向けITサポートも行っています。その業務の中で船上のIT機器についてのサポートを行う上で、船上のITインフラ整備が必要になりました。その流れで、船上IT機器監視サービスを展開しようと2017年11月から開発を始めました。サイバーセキュリティでは欠かすことのできないネットワーク監視を陸上から行うものです。昨年から商用運用を開始しております。船舶におけるサイバーセキュリティをどのように考え、対応して行くべきなのか、本稿がその答えを導く一助になればと思っております。

1　そもそもサイバーリスク・サイバーセキュリティとは？

サイバーリスクを考えるのに、「コンピュータ」、「ネットワーク」はつきものですが、コンピュータとは、パソコンだけでなく、機械の中にあるマイコンも含みます。ネットワークは、インターネットだけでなく、LANを含むパソコンやマイコンなどのコンピュータ同士を接続するもの全てを含みます。この基本が船舶では非常に大事なところです。

リスクを2段階に分けて考えてみます。

①コンピュータやネットワークそのものが使えなくなるリスク

②コンピュータやネットワークが使えなくなることに起因して業務に支障が出るリスク

下記事象などが起こるとコンピュータやネットワークが使用できなくなります。

・コンピュータのソフト障害（ウィルス感染

や、ライセンス切れなども。）
・コンピュータのハード故障（若しくは、故障はしていないが、物理的に動かない）
・ネットワーク障害（断線、ハード故障、ソフトウェア不具合）
・コンピュータに保存されているデータ損失・損壊

　また、コンピュータやネットワークが正常に使用できなくなることにより会社が下記損害を被ります。
・コンピュータに保存しているデータが活用できずに業務が滞る。
・経理システムを導入している場合、経理・決算業務や、決済業務が滞る。
・e-mailが使えず、タイムリーなコミュニケーションが取れない。
・なりすましメールや踏み台になってしまい、他社のコンピュータに障害を与えてしまう。

　これらが起こると企業活動そのものが停滞したり、他人に対し直接損害を与えてしまう可能性もあり、経済的ロスを被ります。これらは主にパソコンにおいて起こり得るものですが、機械に入っているマイコンに対して機能不全が起きた場合、工場のラインが止まるなどのことにより当該企業に損失をもたらします。

　サイバーリスクというものは、このようなリスクです。単に壊れたコンピュータを復旧させるだけではなく、滞った日常業務や場合によっては信頼回復の為の時間とコストもリスクとして捉えるべきです。

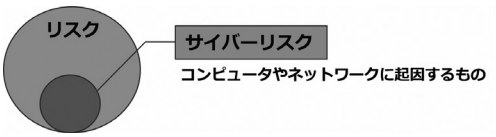
　サイバーセキュリティとは、コンピュータやネットワークが使えなくなるということがないようにする、すなわち、コンピュータやネットワークを堅牢とさせること、また、更にコンピュータやネットワークが使えないことによる損害を防ぐ、ミニマイズすることもセキュリティと言えます。いくらコンピュータやネットワークを堅牢にしたとしても運用する人たち次第で脆弱なものになってしまいます。サイバーセキュリティ対策というと、コンピュータ・ネットワークのハードそのものや、それらの中に導入されているソフトウェアに対して対策を行うと考えがちですが、運用面での体制やマニュアル作りも大変重要です。

2　船舶管理におけるサイバーリスク、サイバーセキュリティ

　世間一般のサイバーセキュリティ ≠ 船舶管理におけるサイバーセキュリティ

　世間一般のサイバーリスク／サイバーセキュリティと船舶におけるサイバーリスク／サイバーセキュリティは、違うと言えます。世間一般のサイバーリスク／サイバーセキュリティは、情報の取り扱いを中心に、特に情報漏洩に関するものと考えられていると言っても過言ではないでしょう。情報処理推進機構がまとめた2019年度情報セキュリティ10大脅威においても多くが情報漏洩事象となっています。ところが、船舶管理においては、情報漏洩だけを考えていれば済むというものではなく、船を運航する、荷役を行うという船やそれに付随する機器をオペレーションするという観点を忘れてはいけません。そのオペレーションを行う上でコンピュータやネットワークを活用することから、それらコンピュータやネットワークが想定通り機能することを担保せねばならない、ということです。

①　船・荷物・船員の安全確保
②　経済的な航海・荷役の実現



この二つは、船長の使命、船舶管理者の使命とも言えます。そして、これらを実現困難とさせる事象をリスクと考えれば、そのリスクの内コンピュータやネットワークに起因するものを船舶におけるサイバーリスクと考えられます。

ある船主さんが、「自分たちには特段盗まれて困るような情報やデータは無いので、サイバーセキュリティは別段考えなくても良い」とおっしゃっていました。それは、情報漏洩という観点だけを考えれば確かにその通りです。しかし、リスクは情報が盗まれるだけではないということを認識すべきです。

情報の取り扱いは、情報システム、いわゆるITです。船舶オペレーションは、制御システム、いわゆるOT（Operational Technology）によるものです。

ある船主さんが、うちはまだFBBだし、インターネットを使わないので、サイバー対策は不要だろうとおっしゃいます。インターネットを介するものに関してはその通りですが、OTについて、そのように言いきれますでしょうか？

制御システム系がインターネットと繋がっているかどうか、それにより船外から船内への侵入懸念があります。インターネットと繋がっていなくとも、内部から不正にアクセスが可能かどうかということを検証する必要があります。

船のオペレーションとサイバーがどう関連するのか？

① IT系

・e-mailが使えなくなる→陸上との交信が途絶え、情報発信や入手ができなくなる
・コンピュータに保存されているデータが活用できなくなる
・船上のコンピュータがウィルスに感染し踏み台となる

②OT系

・ECDISなどの航海計器やVDR、ローディングコンピュータなどの機器がパソコンやインターネットに接続されている場合、それらの機器自体が使用できなくなったり、データが壊れてしまって役に立たなくなる。
・荷役設備や航海機器が機能不全に陥る
インターネットに繋がっていない場合、リスクは低くなりますが、内部からの不正アクセスも想定されます。

3　船舶サイバーセキュリティ対策を求める４つの要素

2017年６月に開催されたIMO第98回海上安全委員会（MSC決議）にて、2021年１月１日以降、最初のDOC年次審査までに、サイバーリスクが安全管理システム（ISMコード）で適切に対処されていることが推奨されました。これはあくまで推奨ですが、船舶管理者がサイバーセキュリティをその管理システムに盛り込むことが要求されたわけです。強制化されるかどうかは、旗国次第となっています。ところが、10月27日に米国が、米国に寄港する船舶に対し、この要件を強制する旨のVessel Cyber Risk Management Working Instructionが発行されました。2021年１月１日以降最初のDOC年次審査までに対応しなければならなくなりました。これはとても大きなことだと思います。

サイバーセキュリティは、安全に関わること、オペレーションに関わることです。例えルール化されていなくとも、対応・対処せねばならないものです。今そこにある危機を認識し、その危機を排除する努力をしなければなりません。また、バラスト処理装置の場合には、その装置をつけるという物理的な事象が要件ですが、サイバーセキュリティには、ゴールがありません。サイバーセキュリティ

は、ここまでやれば良いと言い切れないのです。ルールを満たしていても、技術によって次の瞬間にセキュリティが破られてしまっては、そのルールは陳腐化してしまうからです。

船主・船舶管理会社がサイバーセキュリティ対応をせねばならなくなる要素として、ルール、保険、港、荷主の４つが考えられ、サイバーセキュリティの必要性にドライブをかけています。

＜ルール＞

サイバーセキュリティ対策が堪航性の要件となって行くのか。サイバーセキュリティ対策が取られていない船は船として認めないとなるかです。

＜保険＞

サイバーセキュリティが堪航性にかかわってくるとなると、保険条件の根本に関わってきます。保険については、サイバーリスクが免責となるのかどうかがまず議論になります。現在、本邦の損害保険会社は、船体保険においてサイバーリスクを免責としていません。事故がたとえサイバーリスクに起因するものであったとしても、保険でカバーされるのです。ところが、海外では、既に免責となっているそうです。再保険市場が免責ということは、いずれ、本邦の損害保険会社も免責にして行かざるを得ないと見ています。

＜港＞

港を出入りする船舶がサイバーリスクに晒されていることは明白です。サイバーセキュリティ対策ができていない船舶が、サイバーアタックや何等かの事由により港内で航行不能に陥ったり荷役装置・係船装置がコントロールできなくなるなどの事象、また、単純に港側と通信できなくなるなどの事象が起きた場合、港内の航行中・停泊中の他船舶や港湾設備を危険に晒すことになります。少なくとも、港側は、船舶そのものが危険若しくは他船舶に危険をもたらすものなのかどうかを判断し、対処するということになるべきだと思います。米国がいち早く対応したと言えます。

＜荷主＞

港は、公けの立場でそこを利用する関係者の危険を排除する義務があると思いますが、荷主は、船上にある貨物を確実に目的地に運ばねばなりませんし、受け取らねばなりません。大事な貨物を預ける場所が危険に晒されているのです。預かったものがその危険を認識し、排除する努力をしているのかどうか、当然荷主としては、確認すべきでしょう。船舶のオペレーションまで行かずとも、貨物情報の取り扱いということにおいても荷主は関心高くしていることと思います。誰から受けた、どれほどの貨物が誰向けにどこで引き渡されるのかといった情報を船舶は持っています。その情報がざるの如く漏れてしまってはいけません。OCIMFオシモフ（石油会社国際海事評議会）やRight Shipにおいて船舶のサイバーセキュリティ対策を検査する流れになっています。

４つの立場それぞれがサイバーセキュリティを求めていることになっていますが、今後それぞれがその要求度を強めて行くでしょう。

４　船級の状況

我々日本人にとってやはりClassNKの動向は気になりますし、彼らのサイバーセキュリティに対する考え方や求めていることを整理することで、何をすべきかの方向性も見えてきます。

ClassNKがガイドラインを策定するにあたり、基本的な考え方として「ClassNKサイバーセキュリティアプローチ」を公表しました。

その第一に掲げたのが、「最重要事項は安全運航の確保」です。

また、「継続的な見直しと最新化」も謳っています。他のルールと大きく違うのは、サイバー対策には終わりが無い、ゴールが無いということです。ここまでやればオーケーとは誰も言ってくれません。ある程度はやっておき、それを日々維持・改善して行かねばなりません。「継続的」に、管理策や教育などを「見直し」た上で「最新化」していかねばならないのです。本当に船主泣かせな事だと思います。

この考えに基づいて3つのガイドラインが昨年発行されました。

①「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」

2020年7月に第2版が出ました。ClassNKとしてノーテーション「CybR-G」を付与するとしています。第1版は何が何だかよくわかりませんでした。これは、元々参照していた2018年11月にIACSが公表したRecommendationsが12あって、読み解くのが難しかったのです。今回、IACSが今年5月4日にこれら12個の推奨事項を1つにまとめました。ClassNKはこの一つになった推奨事項、IACS Recommendations, No.166をベースに「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」を作成しています。当ガイドラインは新造船を対象としていますので、新造船を設計・建造するにあたって盛り込まねばならないサイバーセキュリティ上の要件をRec. No.166に基づいて記載しています。この「CybR-G」については、コンピュータシステムおよび船内ネットワークが対象ですので、竣工後の年次審査および臨時審査において求められる状態を維持して行かねばなりません。このガイドラインは新造船が対象とされていますが、既存船でも非常に参考になります。キーワードが三つあります。一つ目

出典元：日本海事協会

が、コンピュータ機器リスト。パソコンのみならず、本来は船用機械に搭載されているコンピュータ全てが対象になりますが、サイバーセキュリティの観点で行けば、ネットワークや物理的に誰かがアクセスして、書き換えることができる機器かどうかで切り分けてしまい、そのような機器だけをリスト化するということになります。次に、ネットワーク論理構成図。船内ネットワークを構成している機器類がどこにどのように接続されているのかをまとめたものです。そして、三つ目が、セキュリティ脆弱性を検証するリスクアセスメント。これら三つのことが要求されています。船舶におけるサイバーセキュリティ上、非常に重要な要素だと言えます。

②「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」

デザインガイドラインは、船舶そのものが対象ですが、このガイドラインでは、船舶管理システム上サイバーセキュリティ対策をどのように考えて盛り込むべきかを示すものとなっています。ISMコードの流れに沿いながら、ISMS（情報セキュリティマネジメントシステム）を適用させてCyber Security Management System（CSMS）を構築するということになると思います。要するにサイバーセキュリティにおける会社としての考え、船舶管理上のルール、運用方針を定め、それをどのように個船に適用させ、維持して行くのか、社員、船員の教育を含めたものとなって行きます。

③「ソフトウェアセキュリティガイドライン」

本船上の個々の設備・機器においてコンピュータシステムと連動若しくは、コンピュータシステムを含んでいる場合、個々の設備・機器においてサイバーセキュリティ対策を施すというものです。これは、船用機械メーカーにて対応してもらうものとなります。

5　求められる対応（CSMSの策定、本船上での対応）

サイバーリスクの世界では、100％リスクを排除することは不可能というのは常識となっています。コンピュータ、ネットワークを堅牢化することは大事ですが、100％は無理です。できるだけ防ぐ努力をし、万が一何か起こった場合の対処法を準備しておくことが大事です。これは、リスクマネージメントの基本です。

少しずつでも対策を講じることでリスクを軽減できます。その努力の継続が大切です。

ISMコードにおいてサイバーセキュリティを盛り込むことがIMOでは求められておりますが、ClassNKでは、サイバーセキュリティマネジメントシステム（CSMS）認証を出しています。ISMコードにサイバーセキュリティを盛り込んでも、新たに認証が追加されることはありません。会社や船がサイバー対策を講じていると言っても、いちいち現場で説明しなければなりません。CSMS認証を取得しておけば、一目瞭然ということです。

CSMS取得では、情報セキュリティ基本方針策定、情報資産洗い出し、情報セキュリティ上の脆弱性検証＝リスクアセスメントの実施、運用ルール・マネジメントシステムの作成をし、この運用ルール・システムが的確に実施できるよう教育します。業務遂行上不具合があれば、是正して行きます。これら一連の作業を行い、審査を受けて晴れて認証取得となります。本船に対する管理策、本船側で実施されるものも含めたものになります。

会社にITの担当者がいたとしても、一筋縄では行かないと思います。今、我々は、ClassNKとも種々話をしながら、できるだけ

シンプルに取得できるよう検討していますが、マリンネットなどの専門家のコンサルティングを受けられることをお薦めします。

本船における対応では、リスクアセスメントが重要となります。IT部分、OT部分に分けて対処して行きます。IT部分では、通信機器、パソコンがインターネットや船内LAN上どのように繋がっているのかを把握します。OTに関しては、ネットワーク化されITと接続できるようになっているか、また、各機器にUSBポートなど外部機器が接続可能かどうかを検証します。各機器リスト及びネットワーク論理構成図を作成します。これが非常に大事です。

そして、IT機器を監視することで状態を把握し、ネットワークを維持管理できることになります。クルーは頻繁に交代しますので、IT機器使用ルールの徹底、また、状態把握は容易ではなく、この運用徹底、状態把握の為にネットワーク監視を行います。これは陸上ではサイバーセキュリティとして確立されているものです。また、重要な要素としてネットワークにおけるデータログを取得しておくということも良く言われています。

ネットワーク監視とデータログ。CSMSを維持して行くためにこれらは必要です。

6　まとめ

船舶におけるサイバーセキュリティ対策は、通常のルール対応とは違い、安全に直結するだけでなく、それを常時維持して行かねばならないし、そのクライテリアが定まっていません。一度対応したら終わりというようなルール対応とは違うということ、また、情報漏洩対応だけでなく、常にオペレーションへの影響に配慮した対応でなければいけないということを忘れないでおいてください。

冒頭にあげました―座礁した船舶はサイバーインシデントではない―と言い切れるか？

ここまで説明して来ましたリスクアセスメントを実施し、本船上のネットワーク監視を行えば、サイバーインシデントの調査が可能になります。本船の航行に重要な事象をもたらすようなサイバー異常があったのかなかったのかをわかるようにするというのが、このCSMSの１つの目的にもなっています。

海事産業はIT化が遅れた産業と言われています。ただし、だからこそ無駄なくIT化を推進できるはずです。IT化を先んじた様々な業界の成功例の中から価格もこなれた優れたものを取捨選択して導入すれば良いのです。そして、セキュリティ対策も同様です。IT化の途上にあるからこそ、できるところから少しずつ手掛けることができます。船上のIT化はまだまだです。船員のITリテラシーも低いと言えます。かえって一からというかゼロから思うように立ち上げれば、現場で運用可能な必要最小限のIT化から効率よく発展させていくことが可能になると考えられます。ITインフラを整備構築し、サイバーセキュリティを確保して、ITを活用した競争力ある船舶になって行くことを願っています。

（筆者略歴）
1990年　早稲田大学理工学部機械工学科卒
1990年　伊藤忠商事株式会社船舶・海洋プロジェクト部入社
2016年　マリンネット株式会社出向、現職
海外駐在　2005～2008年シンガポール、2013～2016年リオデジャネイロ