サイバーリスクと船舶保険

東京海上日動火災保険株式会社
海上業務部船舶業務G　課長代理　金子剛大

サイバーリスクの特徴

リスク自体が日々変化している
- サイバーリスクは新しい攻撃方法または関連技術、参加者により絶えず変化している

人的要因に大きく左右される
- サイバーリスクは内部や外部攻撃者の過失や悪意等、人的要因に大きく左右される

過去の事故データが不足している
- サイバーインシデント関連情報を収集する仕組みがなく、事故データが不足している

大規模な集積損害になる可能性がある
- 多くの組織が同種のクラウド、ソフトウェア、セキュリティプログラム等を使用する傾向

サイバーリスクを理解する

サイバーリスクの特徴：　全体像が分からない

全体像の分かりにくさ…専門用語が多く、報道等では攻撃の対象、攻撃の手法、被害内容等が混在

<サイバー攻撃に関する用語例>
DDoS攻撃、ランサムウェア、APT、ボットネット、マルウェア、ゼロデイ攻撃、標的型攻撃、踏み台、水飲み場型攻撃…etc.

企業の経営・リスク管理にしてみれば、まずは被害内容の観点で整理することが望ましい
被害内容は下記4種類とこれらの組み合わせ*しかない

- 窃取・漏えい
- 改ざん
- 麻痺
- 破壊

＊ ただし、サイバー攻撃は上記の組み合わせであることが多い。例えば、標的型メール攻撃でシステム部門のアクセス権限を盗み、そこからウェブサーバを改ざんし、ウェブサイトを訪問した人の端末にマルウェアをダウンロードさせ、ソフトウェアを破壊するなど。

サイバーリスク（窃取・漏えい）

個人情報漏えいの事例（内的要因）

日時	概要
2019/01/17	原発広報誌の返信ハガキが所在不明、個人情報や意見など記載 - ●●
2019/01/16	学生の個人情報含むPCが海外で盗難被害 - ●●大
2019/01/15	オンラインストアの挨拶状で誤送信 - ●●
2019/01/15	「●●」英語版アンケートで個人情報が閲覧可能に
2019/01/15	PC出張サポート申込者の個人情報が閲覧可能に - ●●
2019/01/15	特別支援学校で生徒の個人情報が所在不明 - ●●
2019/01/11	学生向けのメールで誤送信が相次いで発生 - ●●大
2019/01/10	フィッシング被害でスパム送信、情報流出の可能性 ●●大
2019/01/08	溶解処理する書類を運搬中に紛失 - ●●
2019/01/08	フォーム送信情報を誤送信、サンプルメアドへ - ●●協会
2019/01/07	レターパックで送付した妊婦や乳児の健康診断受診票が所在不明
2019/01/07	市営住宅入居者の個人情報含む台帳を紛失 - ●●市
2019/01/07	通販サイトで個人情報を誤表示、プログラム不具合で - ●●
2019/01/07	患者情報含む書類が車上荒らしで盗難 - ●●大付属病院
2018/12/27	メール誤送信で顧客のメアド流出 - ●●
2018/12/27	ふるさと納税者の個人情報を同意なしで公開 - ●●町
2018/12/27	メール誤送信で卒業生などのメアド流出 - ●●大

出典:個人情報漏洩事件・事故一覧、Security NEXT（2019年1月22日時点）
http://www.security-next.com/category/cat191/cat25?page=51

個人情報漏えいの事例（外的要因）

<政府系機関>

事故公表日時：2015年6月1日
流出情報件数：125万件
流出原因：標的型メール攻撃

<大手旅行代理店>

事故公表日時：2016年6月14日
流出情報件数：793万件
流出原因：標的型メール攻撃

サイバーリスク（窃取・漏えい）

ClassNK Consulting Service

サイバー攻撃による機密情報漏えいの重大性

- 近年、サイバー攻撃による機密情報（技術情報・特許情報・研究開発情報、顧客情報、経営戦略等）の窃取が注目されている。この問題は、米中間などで外交問題化している。
- 注目されている理由の1つは、窃取される情報量がかつてないほど膨大である点である。例えば、ある国の政府系組織は単一の攻撃対象から6.5TBのデータを窃取した(*)。これは、平均的な新聞紙朝刊の約20,000年分に相当する。

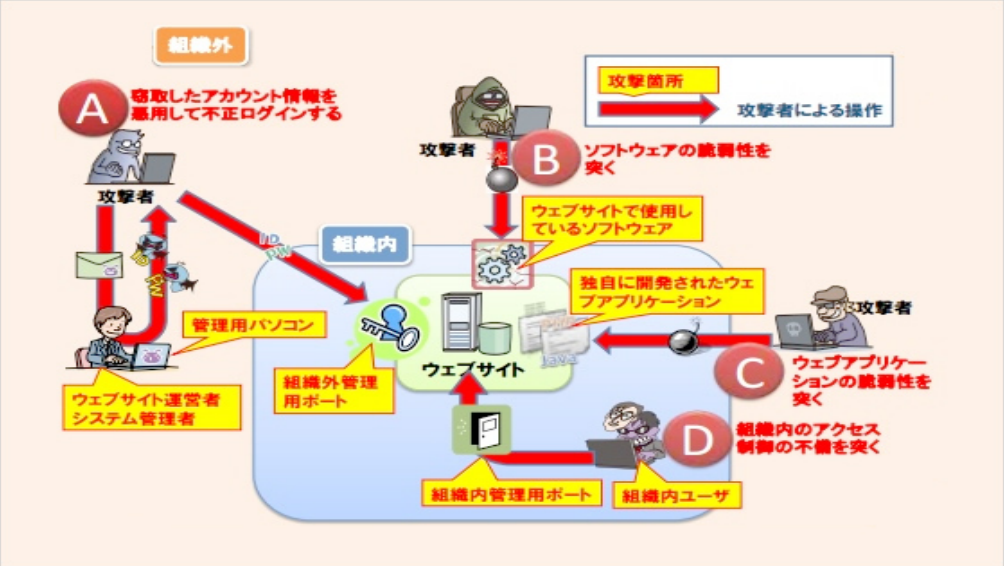
* Mandiant, APT1: Exposing One of China's Cyber. Espionage Units (February 2013)

報道年	事件名称
2009年3月	**GhostNet** …カナダ・トロント大学、英・ケンブリッジ大学の共同研究プロジェクト・チームの研究結果によれば、世界103か国以上で1,295台以上のコンピューターがボット化（攻撃者の統制下におかれ、コンピュータが操作される状況）していた。
2011年3月	**Night Dragon** …2009年11月より、石油・エネルギー業界を中心に、社内文書、石油・ガスの取引情報、プロジェクトファイナンス情報などが攻撃対象となっている。マカフィーによれば、これらは中国発の攻撃である。
2011年10月	**化学・防衛産業の知的財産への攻撃** …化学・防衛産業を中心とする48企業に、少なくとも6か月間のサイバー攻撃が行われた。シマンテックによれば、河北省のコンピュータから攻撃が行われた。
2012年3月	**NASAへの攻撃** …NASA職員150名以上のアカウント情報が盗まれ、中国のIPアドレスからロケット推進研究所（Jet Propulsion Laboratory ）が攻撃を受けてフルアクセスを許した。
2014年5月	**米重工会社へのサイバー攻撃** …新型原子炉の設計等に関する情報が盗まれた。

サイバーリスク（改ざん）

ClassNK Consulting Service

Webサイト改ざん



A: 管理者のID・パスワードが盗まれ、攻撃者が管理者として実行するWebサイトの改ざん

B: WebサイトのソフトウェアやWebアプリケーションの脆弱性を攻撃して実行する改ざん

C: 外部からの脆弱性攻撃やSQLインジェクションによって入り込んで実行する改ざん

D: 組織内部からの改ざん

IPA（独立行政法人 情報処理推進機構）によるWebサイト改ざんの手口の解説図
IPA（独立行政法人 情報処理推進機構）
「Webサイト改ざんの脅威と対策～企業の信頼を守るために求められること ～」
https://www.ipa.go.jp/files/000041364.pdf

サイバーリスク（麻痺）

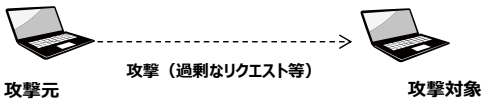
ClassNK Consulting Service

DoS攻撃とDDoS攻撃

- DoS攻撃とDDoS攻撃の違いは、攻撃元が単一か分散しているかである。DDoS攻撃の場合、攻撃元が分散しているため、対処が難しく、真の攻撃元を特定しにくい。

DoS攻撃
（Denial of Service attack）

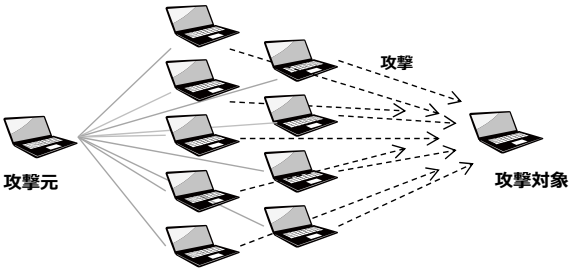
- 対象のサーバや回線に過剰な負荷をかけ、サービスの正常な提供を妨害する攻撃。



※サーバ等も便宜上、コンピュータ端末として図示している。

DDoS攻撃
（Distributed Denial of Service attack）

- DoS攻撃のうち、攻撃元がネットワーク上に分散している攻撃。マルウェア等に感染した数多くのコンピュータ端末から攻撃が行われることから、対処が難しく、真の攻撃元を特定にしにくい。

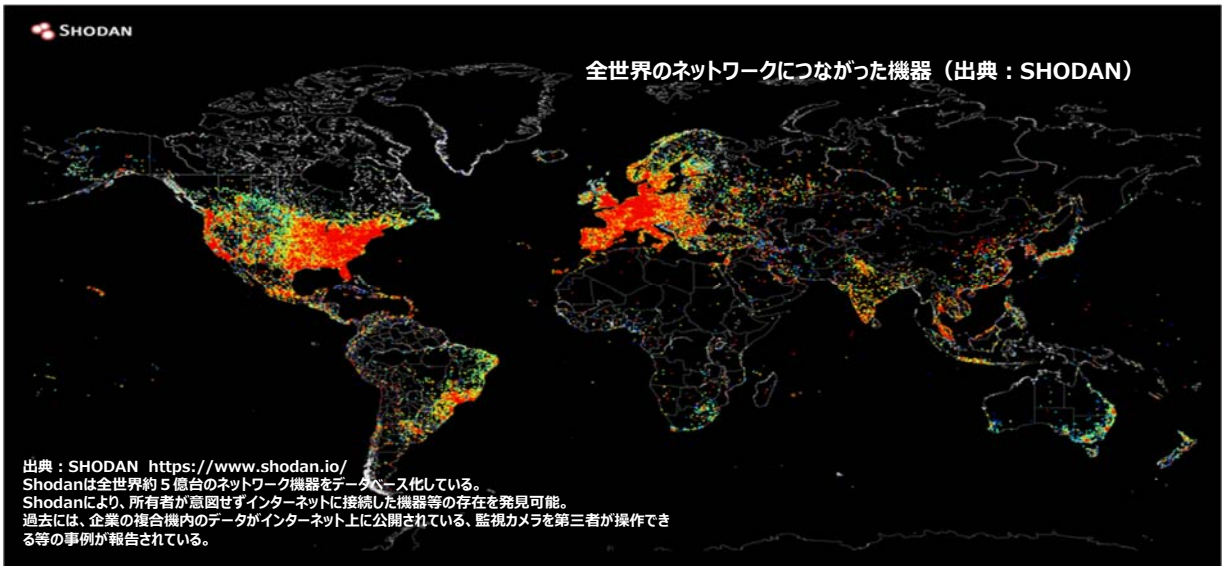


サイバーリスク（破壊）

ClassNK Consulting Service

身の回りの家電製品・オフィス機器へのサイバー攻撃

- 「モノのインターネット（IoT: Internet of Things）」化の急速な進展により、ネットワーク接続機器（家電製品、オフィス機器、電気メーター、自動車（connected car））へのサイバー攻撃が懸念されている。



サイバーリスク（破壊）

ClassNK Consulting Service

社会インフラを狙ったサイバー攻撃の実例

原発の制御システム停止（米国、2003年）

発電所の制御システムがウィルスに感染。制御システムが約５時間にわたって停止。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが製鉄所の制御システムに侵入し、不正操作をしたため、生産設備が損傷。

石油パイプラインの爆発（トルコ、2008年）

何者かが石油事業者のネットワークに侵入。パイプラインの圧力を高めて爆発。

変電所へのサイバー攻撃（ウクライナ、2015年）

マルウェアの感染により、変電所が遠隔制御された結果、数万世帯で3～6時間にわたる大停電が発生。

ロンドン五輪への攻撃（イギリス、2012年）

毎秒約１万件の不正通信。開会式会場の電力システムへの攻撃情報。手動に切り替え。

サイバーリスク（その他）

ClassNK Consulting Service

ランサムウェア（Ransomware）

感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラム（身代金要求型不正プログラムとも呼ばれる）

スパムメールや、改ざんした正規サイトから、脆弱性を攻撃する不正サイトへ誘導され感染する。ランサムウェアが活動開始すると、感染PCの特定機能を無効化し操作不能にする、もしくは、データファイルを暗号化し利用不能にする、などの活動が行われる。PCを感染前の状態に戻すことと引き換えに金銭の支払いを要求する画面が表示される。

出典　トレンドマイクロサイト
http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/ransomware/index.html

サイバーリスク（その他）

ビジネスメール詐欺（BEC）

巧妙な騙しの手口を駆使した、偽の電子メールを組織・企業に送り付け、従業員を騙して送金取引に係る資金を詐取するといった、金銭的な被害をもたらすサイバー攻撃です。詐欺行為の準備として、企業内の従業員などの情報が狙われたり、情報を窃取するウイルスが悪用されることもある。

＜BECの５つのタイプ＞

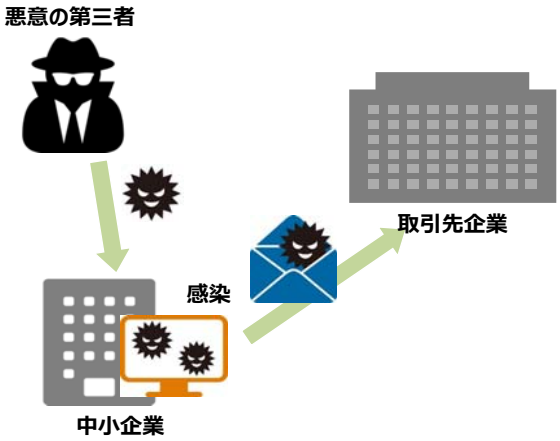
①取引のメールの最中に割り込み、偽の請求書（振込先）を送る
②経営者を騙り、偽の振り込み先に振り込ませる
③メールアカウントを乗っ取り、取引先に対して詐欺を行う
④社長から指示を受けた弁護士といった人物になりすまし、振り込ませる
⑤経営層や人事部になりすまし、今後の詐欺に利用するため、社内の従業員の情報を 詐取する

出典 ビジネスメール詐欺「BEC」- IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/files/000068781.pdfl

サイバーリスク（その他）

踏み台

標的企業の守りが堅い場合、標的にたどり着くため、サイバー攻撃者は周辺企業から攻撃を仕掛けることは珍しくない。標的企業の取引先サイトに侵入したり、知人のアカウントを乗っ取ったりすることで攻撃のための情報を窃取することもあれば、知人になりすましてマルウェアを送り込むこともある。
企業（特に中小企業）は、単純に侵入しやすいという理由で、DDoS攻撃やマルウェア配布に利用する「踏み台」として狙われることがある。企業は、侵入された被害者であるはずなのに、取引先や一般ユーザーに対して加害者になってしまうといった事態になりかねない。



IoTによって変わるリスク

ClassNK Consulting Service

IoT技術によってリスク軽減が期待されていますが、一方で、損害を引き起こす原因の種類は増えます。IoT事業者は新たなリスクを把握し、対処する必要があります。

IoT導入前のリスク

- 衝突事故・座礁事故
- 予期せぬ機器故障による利益喪失
- 人為ミスによる主機停止

IoT導入による※ リスク軽減
※ビックデータ解析、障害予知

IoT導入後のリスク

- (危険予知による早期避航で事故回避)
- (故障予知による適切な時期の機器メンテナンス)
- (操業監視、自動制御による人為ミス低減)

IoTセキュリティリスク

- サイバー攻撃による 運航の停止、不正操作や情報漏えい
- 危険予知機器発動による 機器損壊前の操業停止、利益喪失

IoT導入によって増えたリスク

物理的な機器がITと繋がることにより、従来のリスク(安全性等に係るリスク)に加え、サイバーセキュリティに係るリスクへの対処も必要となります。

サイバーリスクを補償する保険商品

ClassNK Consulting Service

要因	損害の形態	主な損害		対応する保険商品
サイバー攻撃	物的損壊を伴う損害	自社への補償	沈没・座礁・火災・衝突	船舶保険
			機器損害	
			その他物的損傷	
		第三者への補償	衝突損害賠償責任	P&I保険
			港湾施設の損害	
			その他賠償責任	
	物的損壊を伴わない損害	自社への補償	費用損害	サイバーリスク保険 個人情報漏えい保険 役員賠償責任保険（D＆O）
			データ損害	
			利益・営業継続費用	
		第三者への補償	賠償責任	
			情報漏えい	
			見舞金	

船舶保険におけるサイバー危険免責

ClassNK Consulting Service

Cl.380 Institute Cyber Attack Exclusion (01/11/2002)

1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

- ✓ 平時のサイバー攻撃による損害を全面的に免責とするもの（通称：Cl.380）。
- ✓ 戦争保険に付帯される場合には、コンピューター制御ミサイル等による損害を復活担保する。

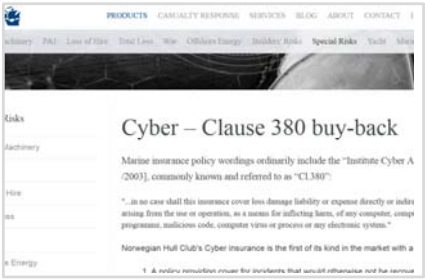
ロンドンの船舶保険マーケットにおいては普及しつつあるが、本邦船舶保険においては未導入。

サイバー免責の復活担保の動き

ClassNK Consulting Service

Norwegian Hull Club

"Clause 380 buy-back"



SIGCo

"Cyber Hull Cover"

Beazley

"Cyber Defence for marine"

いずれの商品もCl.380等のサイバー免責規定によりてん補されない船舶の損害を復活担保するもの。

保険会社の課題

- リスク量の把握
- 集積コントロール
- 再保険調達
- 事故原因の分析技術
- 海運業界のサイバーリスク耐性向上への貢献
  - ✓ サイバーリスクマネジメントへの専門性向上
  - ✓ サイバー認証取得の促進
  - ✓ 事故事例の収集

ご清聴ありがとうございました。

サイバーリスクと船舶保険

1. はじめに

　デジタル技術が飛躍的に発展する一方で、近年のサイバー攻撃もまた著しく進化しており、日々刻々と新たな脅威が発生している。海運業界においても、IoT 技術の普及によって船舶に対するサイバーリスクは増加の一途を辿っており、船舶保険者としても大きな関心を寄せる分野となっている。本講演では、一般論としてのサイバーリスクを概観しつつ、船舶保険における国際的動向および船舶保険会社が抱える課題を整理する。

2. サイバーリスクの理解

　サイバーリスクの特徴の一つが、「全体像の分かりにくさ」である。日々複雑化する攻撃内容に加え、攻撃の対象や手法、被害内容も多様化しており、かつそれらに関する専門用語が混在していることが、その分かりにくさを助長していると言える。

　このように全体像が掴みにくいサイバーリスクについては、まずは被害内容の観点で整理することが理解への近道である。実は、一見複雑なサイバーリスクは、大きく分けて「窃取・漏えい」・「改ざん」・「麻痺」・「破壊」の４種類とこれらの組み合わせしかないと言われており、数多くの複雑な攻撃手法も、被害内容で分類することで単純化して整理可能である。

　例えば、「窃取・漏えい」としては、個人情報漏えいや企業機密情報漏えい、「改ざん」としては Web サイトの改ざんが挙げられる。その他、DoS 攻撃は「麻痺」を狙った攻撃の一例であり、製鉄所や石油パイプライン等の社会インフラの「破壊」を狙ったサイバー攻撃もこれまでに数多く確認されている。

3. IoT によって変わるリスクと保険

　IoT 技術の進歩により、危険予知・故障予知の精度が大きく高まり、その結果として海難事故や機器故障の発生リスクの軽減が期待されている。しかしながら、従来型の安全性に係るリスクが減少する一方で、サイバーリスクについては、IoT 技術の進歩がかえってリスクを増加させることとなるため、企業としては、こうした新たなリスクにも目を向け、全体像を把握したうえで、適切な対処を実施することが求められている。

　リスクコントロールの手段としては、一般的に「保有」「低減」「移転」「回避」などがあるが、サイバーリスクのような、仮に発生した場合の影響（損害）が大きいリスクについては、最も有効なリスクコントロール手段が、保険を用いたリスク「移転」であると言われている。なお、サイバー攻撃を原因とした損害については、当社では大きく分けて物理的損傷を伴う損害を従来の船舶保険で、物理的損傷を伴わない損害をサイバー保険等で対応している。

4. サイバー危険免責をめぐる動き

　前述のとおり、仮にサイバー攻撃が原因であっても、船舶に物理的損傷を伴う場合の損害については、サイバー攻撃以外を原因とする損害と同様に、通常の船舶保険でてん補するのが、当社を含め本邦の船舶保険会社の基本的なスタンスである。

　一方で、ロンドンを中心とした国際船舶保険マーケットにおいては、21 世紀に入った頃より、

サイバー危険免責の導入が進んでおり、現在では通称「Cl.380」と呼ばれるサイバー危険免責条項が船舶保険約款に導入されるケースが一般的になりつつある。すなわち、国際船舶保険マーケットにおいては、サイバー攻撃による本船の損害は、たとえ物理的な損傷を伴っていたとしても、こうした免責条項に基づきてん補されない状況にある。

こうした環境下、近年では複数の保険会社がサイバー危険を復活担保する保険商品の開発にも乗り出している。その中には、船級協会による事前のリスクアセスメントなどを引受条件とし、保険の提供を通して契約者となる船会社のサイバーリスク耐性向上を目指して取り組む保険会社も存在する。

いずれにせよ免責規定が導入されていない本邦船舶保険会社に加入する船会社にとって、現時点でこの復活カバーは必要性がないものではあるが、船舶保険を通じて船会社のサイバーセキュリティを向上させようという取り組みは、注目に値するものと考える。

5. 保険会社の課題

サイバーリスクについて、本邦船舶保険会社が抱える課題としては、第一にリスクの定量化の困難が挙げられる。本来、リスクエクスポージャーの増加は適切に保険料に反映されなければならないが、従来型の統計的な手法では、サイバーリスクのような目に見えず、事故原因としても特定されにくいリスクは、保険料化することが非常に難しい。また、大規模・広範なサイバー攻撃が発生し、事故が集積することも予想されるため、戦争危険や地震危険のような異常危険と同様の慎重な取り扱いが求められる。そして、前述のとおり国際マーケットにおいてサイバーリスクの免責規定が一般化しつつある中、これまでどおりの再保険調達が継続できるかどうかも大きな課題の一つとして認識している。船舶保険はリスクが立体的で再保険への依存度が高い商品であり、仮に再保険条件でサイバーリスクが免責となった場合、本邦船社に提供している元受保険条件もまた、サイバー危険免責の導入を検討しなければならない。

6. おわりに

船舶保険会社として、サイバーリスクの増加は対処すべき経営課題の一つであるが、一方でまた、海運業界のサイバーセキュリティを強化するために如何に貢献できるかというのも、船舶保険会社の社会的使命である。こうした使命を果たすためにも、サイバーリスクマネジメントに関する専門的知見を深め、リスクマネジメントのプロとしてお客様をサポートできる存在を目指すとともに、船級協会等の業界関係機関とも協力し、船社のサイバーリスクマネジメントシステムの構築を支援する仕組みも検討していく必要がある。