JAPAN P&I NEWS

No.944-18/2/20

外航組合員各位

サイバーリスクとサイバーセキュリティ（その2）

このサーキュラーは、サイバーリスクとサイバーセキュリティの問題について最新情報を組合員の皆さまにご案内するもので、本稿はその第二弾です。１１月１０日掲載の第一回ではサイバーリスクの概要をご案内しました。今回はサイバーセキュリティに関する国際規則や指針を説明し、次回はサイバー攻撃の事例紹介を予定しています。

サイバーリスク：規則と指針

海運業界では、それぞれの船社と船舶の状況に応じてサイバーセキュリティ対策を行うべきだと認識されています。例えば、ごく限られた電子システムしか搭載していない船舶は、相互に複雑に接続された電子システムを搭載する船舶と同レベルのリスク分析をする必要はないということです。

ＥＵと米国ではサイバーセキュリティのルールを作成中ですが、国家的・国際的なルールは現在殆どありません。そのようなルールが完成するまでの対応として、BIMCO などの海事団体が、この複雑な新領域でメンバーに指針を与えるためにサイバーセキュリティの手引きを作成しました。

BIMCO のガイドライン

BIMCO はここ数年、船上の電子機器増加に伴うリスクの増大について議論をリードしており、2017 年には、2016 年の船上のサイバーセキュリティガイドライン「2016 Guidelines on Cyber Security Onboard Ships」の改訂版を発行しました。同ガイドラインについては、国際海運会議所（ICS）、インタータンコ(Intertanko)、インターガーゴ(Intercargo)、クルーズライン国際協会（CLIA)が支持を表明しています。

改訂ガイドラインは、近年、BIMCO が蓄えてきた知識と経験に基づくもので、現在、海運業界にとって最も包括的なガイドラインと見なされています。

世界の船舶の６割をカバーする BIMCO は、同ガイドライン作成のために米沿岸警備隊やリベリア船籍と協力し、海事調査員を BIMCO メンバーの船舶に乗船させて、潜在的なサイバーアタックについての調査を行いました。この調査結果では、他の多くの調査と同様に、サイバーアタックの潜在的可能性が高いことが示されました。

同ガイドラインは船主や運航者に、どのように船舶運航のリスクを査定し、そしてシステムの脆弱性を特定し、どう防御策をとるかについての手引きを提供しています。同ガイドラインは独立したものではなく、ISM コードや ISPS コードに準じた現行の規則の補足として作成されています。

BIMCO はサイバーセキュリティ対策が各船社と船舶に応じたものであるべきだと認識していますが、同ガイドラインは、リスクへの取り組みは適切な基準で推進されるべきとしています。同ガイドラインではサイバーセキュリティの認識で重要となる以下の 6 項目に焦点を当てています。

1. 危険を特定し、船舶へのサイバーセキュリティの危険を理解する。
2. 船舶のサイバーセキュリティシステム内の脆弱性を特定する。
3. 外部の危険に侵入される可能性とリスクの影響度を査定する。
4. 影響を最小限に抑えるための防御策と発見方法を策定する。
5. 危険の影響を減らすための非常事態対応計画を確立する。
6. サイバーセキュリティ事故に適切に対応する。

これらが組合員の皆さまがサイバーセキュリティを査定する際に考えなければいけない点です。当組合では、組合員の皆さまがこれらの問題に対応するために、外部の専門家を起用するお手伝いができます。サイバーセキュリティの査定には以下の諸段階が含まれます。

- 船舶から陸上のインターネットへの接続経路を管理・監視する。
- 船上のネットワークを陸上と分離する。
- 管理されているネットワークと管理されていないネットワーク間の接続を防ぐ。
- 重要なシステムとデータ保護のために複数の保護階層を使用する。
- 効果的なサイバー侵入緊急対応計画を用意する。

組合員の皆さまがリスク分析を実施しリスクが明確になれば、そのリスクは取引先との契約でそのリスクを相手方に割り当てたり、サイバー保険を契約したりすることで、リスクを外部に移転または軽減させることができるかもしれません。組合員の皆さまにおかれては、ご利用の保険ブローカーと、サイバーリスクに関して手当てできる保険についてご相談されることをお勧めします。

IMO ガイドライン

IMO 海上安全委員会は、2017 年 6 月の会合を受けて、サイバーリスク管理についての

新ガイドラインを発行しました。

IMO ガイドラインは、船主や運航者が、それぞれの安全管理システム（SMS）にサイバーリスク管理への考慮が必須であることを示しています。同委員会は、2021 年 1 月 1 日以降に来る最初の年次の適合証書（DOC）の取得時までに、各社の SMS をサイバーリスクに適切に対応させなければならないとし、それに合わせた予定表を提示しました。

もし組合員がサイバー攻撃の被害を受けた際、サイバーリスク管理と本船の保護に相当な注意を払っていたことが示せないと、本船が航海に適している状態でなかったとみなされて運送契約の不履行となるリスクがあります。もし裁判所がこのような判決を下し、調査においても軽率で相当な注意義務を果たしていないとみなされた場合、保険によるてん補に影響が出る可能性もあります。

結論

サイバー攻撃のリスクは増加しています。サイバー攻撃の被害にあった場合、深刻な経済的損失に直面する可能性があります。現在、国家的または国際的なサイバーリスク規制はないものの、BIMCO のガイドラインを含め、海運業界は組合員の皆さまがこれらのリスクから自らを守る対策をとるための包括的な手引きを用意しています。リスクを査定するためにこれらの手引きを検討し、特に最近の IMO のサイバーリスク管理の実施についての勧告に沿って適切な対応を行うことが重要です。

（本サーキュラーは英国の法律事務所 Holman Fenwick Willan LLP (http://www.hfw.com/Home)のマシュー・モンゴメリー氏とジーン・コー氏より当組合にご提供いただきました。）

関連リンク
BIMCO Guidelines on Cyber Security Onboard Ships
IMO GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

以上

日本船主責任相互保険組合