JAPAN P&I NEWS

No.949-18/3/15

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3）

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、本稿はその最終回です。2017 年 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、2018 年 2 月 20 日掲載の第二回ではサイバーセキュリティに関する国際規則や指針をご説明しました。今回は起こりうるサイバー攻撃のシナリオを考察します。

概要

技術は進歩しているものの、海本来の危険、付近を航行する他船やシステム故障などによる安全航行への脅威がなくなることはありません。さらに船上の電子システムの増加に伴い、新たな「サイバー」脅威も認識されています。このリスクは悪質なソフトウェア（マルウェア）や標的型攻撃、またユーザーによるミスなどにより引き起こされます。

シナリオ１：堪航性のない本船？

穀物を輸送していたばら積み貨物船が、電子システムの故障のために座礁。船倉が浸水し、その結果サルベージ作業が行われました。船倉浸水により、貨物の約半分が損傷を受け喪失。船主は共同海損を宣言。安全港に本船を曳航し、荷降ろしをするための費用が発生しました。

システム故障の原因調査により、重要なソフトウェアパッチが電子オペレーティングシステムの一つに適用されていなかったことが判明。座礁前の数ヶ月間、ソフトウフェア製造者が船主のシニアマネージャーの一人に、ソフトウェアパッチ適用の必要性を勧告するメールを繰り返し送っていたことも明らかになりました。同マネージャーはこれらのメールを見落としており、勧告にも従っていませんでした。その結果、本船システムは停電を引き起こすマルウェアの被害を受けやすくなっていました。

貨物関係者は、貨物損害とサルベージ業者に支払う費用に関するクレーム請求をしようとしています。これらのクレームはヘーグ・ルールまたはヘーグ・ヴィスビー・ルールを摂取していると見られる運送契約に従い、船主に対して請求されることになります。

貨物関係者が船主へのクレーム請求を裁判官に容認させるには、本船が出航時点で堪航

性がない状態だったと示す必要があります。イギリス法では、船主が本船を航海に適している状態にするために慎重に行動していたかどうかも、評価の対象となります。船主の行動は、その時点での業界の標準的な知識に照らし合わせて判断されます。BIMCOガイドラインと海運業界のガイダンス（第二回サーキュラー参照）によると、この場合船主は電子ソフトウェアの更新を怠ったとして批判されることになります。

イギリス法では、船主は座礁原因に関する詳細を公表しなければならないことになっています。ソフトウェアパッチを適用しなかったとの証拠があれば、出航時に本船が堪航性のない状態であったと見なされる可能性が非常に高くなります。

船主は、本船が堪航性のない状態だったにも関わらず、自分たちは相当の注意を尽くしていたと主張するかもしれません。しかし、シニアマネージャーがソフトウェア製造業者の指示に従っていないので、そのような抗弁を維持するのは難しいでしょう。イギリス法では、船主の主張は容認されず、貨物関係者が貨物損害とサルベージ業者へ支払った費用を回収できる可能性が高いのです。

さらに、相当の注意を尽くすことを怠ったことにより本船が堪航性を欠く状態だったと認定されれば、船主は貨物関係者から共同海損分担金を回収することはできないでしょう。

P&I 保険はこのようなケースに対応するようになっていますが、組合員の皆さまには、上述のようなクレームが発生した場合に最大限の弁護を行えるよう、サイバーセキュリティ問題に取り組まれることを強くお勧めします。2 月 20 日掲載の第二回サーキュラーでは、船主が達成すべきガイドラインと基準を紹介しています。より詳しい情報が必要な場合はそちらをご参照ください。

シナリオ２：送金詐欺（マンデート・フロード）

当組合では、マンデート・フロード（送金詐欺）被害の増加も認識しています。マンデート・フロードとは、資金が別の第三者の銀行口座に送金されるよう、不正な送金指示を行う詐欺のことを指します。陸上の電子システムが脆弱で、ハッカーが会社のメールをモニターできてしまうことにより起きることがよくあります。例えば、会社とそのサプライヤーのメールのやりとりの中で、サプライヤーになりすましたハッカーが送金指示のメールを会社に送り、サプライヤーの銀行口座でなく、別の口座に振り込まれるようにします。このようなメールは大抵、一見サプライヤーから来たように見えるアドレスから発信されます。よく見ればアドレスの中の一文字だけが違っているという具合です。

このような詐欺の被害を受けないようにするためには、システムのセキュリティを確実にしておくことが大切です。さらに、リスクを最小限にとどめるための手順を決めておくことをお勧めします。例えば、送金前に支払先に電話を一本入れ、銀行口座の詳細を確認するなどの手順です。上述のようなケースの場合は、請求が正しいものか確かめようと受け取ったメールに返信をしたとしても、被害の防止にはなりません。

結論

このサーキュラーシリーズが、組合員の皆さまのビジネスにおけるサイバーセキュリティの重要性を理解する一助となるよう願っております。

（本サーキュラーシリーズは英国の法律事務所 HolmanFenwick Willan LLP (http://www.hfw.com/Home)のジーン・コー氏より当組合にご提供いただきました。ご質問がある場合は当組合またはジーン・コー氏にお問い合わせください。）

以上

日本船主責任相互保険組合