JAPAN P&I NEWS

No.929-17/11/10

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1）

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方々にお知らせするための三部構成のサーキュラーの第一部です。第一部ではサイバーリスクの概要、第二部で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、第三部ではサイバー攻撃の事例紹介を予定しています。

サイバーリスクの概要

サイバーセキュリティは今に始まった問題ではありませんが、最近は国際的なニュースや海運メディアで大いに注目されています。組合員の方々も今年に入って大規模なサイバーセキュリティ侵害を多く耳にしていることと思います。一例を挙げるとマースクがNotPetya と呼ばれるコンピューターウイルスの大規模な攻撃の対象となりました。この攻撃により今年７月にマースクライン、APM ターミナル、ダムコが何週間もの間、業務を妨害されました。

この例でも明らかなように、海運業界はサイバー攻撃リスクへの対処を真剣に考えなければなりません。情報技術と電子システムは海運業界で不可欠な役目を果たしており、主な例としては下のようなものがあります。

- AIS（自動船舶識別装置）は船舶動静や識別データ情報を他船や港湾、沿岸警備隊と交換するために使用されています。

- 船舶の位置と速度は ECDIS（電子海図情報表示装置）に表示されますが、その ECDIS は頻繁にインターネットを通じてデータ更新をおこなっています。

- 船やコンテナ港では船舶位置の把握、クレーン操作、コンテナ積み下ろしのためにGPS（全地球測位システム）情報を使用しています。

このような技術の進歩は一般的に作業の効率向上をもたらしましたが、これらのシステムには悪用される脆弱性があることも明らかになりました。さらに同じネットワーク上で稼動している別の構成部品や相互接続されているシステムへのリスクも高まっており、このような電子システムは慎重に運用され、保護される必要があります。

リスクタイプとその影響を認識

リスクは不適切な運用、技術上の欠陥、訓練不足、システム設計不備により生じるかもしれませんし、または悪意のある意図的な攻撃により生じるかもしれません。もし脆弱性が悪用されれば、セキュリティ、機密性、システム運用、安全を司る重要な機能が損なわれる可能性があります。海運業界では、日常的に高価な貨物が輸送され、高価な資産を保有し、乗客の個人情報を管理するなどハッカーが攻撃を試みる明らかな動機があります。

航海、エンジンコントロール、操船、荷役において海運業界が電子システムやインターネットへの依存を高める中で、船主である組合員の皆さまは特に攻撃の対象となりやすくなってきたと当組合は考えています。そのため組合員の皆さまにはサイバーセキュリティ問題に十分な注意を払うことが必要になります。例えば、古いオペレーティングシステムが使用されていたり、コンピューターシステムに必要な補修がされていなければ、サイバー攻撃のリスクが増加します。システムの脆弱性が高ければ高いほど、ハッカーがそれに乗じて攻撃を試みる可能性が高くなります。

サイバー攻撃による損害の規模を推し量ることは困難です。最近の見積もりではマースクが NotPetya で受けた損害は３億ドル以上にのぼるだろうとしています。また攻撃がその会社のシステムの脆弱性を示したということになれば、経済的な損害のみならず会社自体への評価が損なわれることもあると考えられます。もし貨物が損傷したり又は遅延した場合には損害賠償請求が起こされるかもしれません。最後になりましたが、攻撃が起きた土地の司法権や攻撃の性質によっては罰金命令や裁判を起こされるリスクがあることにも注意が必要です。

サイバーリスク対応

当組合の保険契約規定ではサイバーリスクを特定して述べていませんが、もしサイバー攻撃や侵害によるクレームが起きた場合は保険契約規定に則り通常通りにてん補の可否が検討されます。サイバー攻撃が保険契約規定の第 35 条の「戦争」や「テロ行為」に該当しない場合、組合員は通常の P&I 保険によるてん補の対象となりえます。海運業界のサイバーリスク対応への動きは遅かったと考えられていますが、2015 年以来 BIMCO、IUMI、ICS（国際海運会議所）、Intertanko、最近では IMO（国際海事機関）などの団体がサイバーセキュリティを優先事項としています。P&I 保険におけるサイバー攻撃の定義は、上記の海運団体での議論に国際 P&I グループ（IG）が加わったことで、より明確になるはずです。

とはいえ、組合員の皆さまには、サイバー攻撃の可能性を最小限に食い止めるために、サイバーリスク管理を細心の注意を払って早急に行うことを強く推奨します。

本サーキュラーの第二部では、これまでに発行されたガイドラインや推奨事項をご紹介します。それにより組合員の皆さまがご自分のシステムに潜在的脆弱性があるかを確認するための手段を提供し、サイバー攻撃への対応の仕方を提示したいと考えます。

さらに第三部では組合員の皆さまが受ける可能性のあるサイバー攻撃の事例をご紹介します。電子ソフトウェアをアップデートしなかったことが引き起こした座礁事故、サイバー攻撃者が送金先の銀行口座をすり替えるいわゆる「振り込め詐欺」の事例などをご紹介します。

（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・コー氏より弊組合にご提供いただきました。）

以上

日本船主責任相互保険組合