TOKIO MARINE Topics (物流関連速報)

脅威を増すサイバー攻撃

TOKIO MARINE NICHIDO
東京海上日動火災保険株式会社
（2017 年 9 月 29 日）

本年6月27日に発生した大規模サイバー攻撃によって、物流業界では海運大手 A･P･モラー･マースク社や米国 Fedex 社傘下の TNT エクスプレスが被害を受けました。先日、両社が当該サイバー攻撃によって被った損害額を発表しております。本号では、近年脅威を増すサイバー攻撃と、物流に与える影響に触れます。

1. 史上最大規模のサイバー攻撃

以前の Tokio Marine Topics でも複数回取り上げましたが、2017年6月末に仕掛けられた暗号化型ランサムウェア「PETYA」による大規模サイバー攻撃によって、ウクライナ政府や欧州企業を中心に甚大な被害が出ました。

物流業界への影響も大きく、コンテナ輸送世界最大手の A.P.モラー･マースク社はこのサイバー攻撃によって IT システムが遮断されました。その影響で受注が出来なくなると同時に、運営するインド最大のコンテナターミナル JNPT（Jawaharal Nehru Port Terminal）を閉鎖せざるを得なくなる等大きな混乱をもたらしましたが、今般、その損失額が3億米ドルに上ったと発表しました。

また、米国 FEDEX 社傘下の TNT エクスプレス社も同サイバー攻撃により被害を受け、発送の遅れ等の影響が出ましたが、先般やはり3億米ドルの損失を発表しています。

2. 増え続けるサイバー攻撃

今回のサイバー攻撃で国内企業への直接の被害は報告されていませんが、日本国内でも、サイバー攻撃の脅威は増加しています。国立研究開発法人･情報通信研究機構（NICT）の調査では、2016年の国内でのサイバー攻撃の件数は前年比2．4倍の約1，281億件となり過去最高となったことがわかりました。調査を開始した2005年の同件数が約3．1億件であったことから、過去10年程度で400倍以上増加した事になります。

3. 物流への影響と求められる対策

サイバー攻撃は資金目的である事が多く、その場合、高額な貨物を日常的に大量に輸送する物流業界はサイバー攻撃のターゲットにされやすいといえます。今回のサイバー攻撃で、物流会社が被る被害の大きさが明らかとなったと共に、荷主側でもターミナルの閉鎖により貨物が滞留･遅延する等の間接的な被害が出ました。船舶の運航では GPS を始めとする電子機器が重要な役割を果たしていることから、仮に運航機器にトラブルが生じた場合、更なる甚大な被害が起きないともいえません。物流業界のデジタル化が進む一方で、サイバーリスクへの備えも早急に講じていく必要があります。

◇◆

船舶･貨物･運送の保険の情報サイト「マリンサイト」
http://www.tokiomarine-nichido.co.jp/hojin/marine_site/index2.html