Gard Insight

海事業界のサイバーセキュリティに対する意識

こちらは、英文記事「Cyber security awareness in the maritime industry」（2016 年 10 月 31 日付）の和訳です。

サイバーリスクをすべて管理できる単一の解決策は残念ながらありません。サイバーリスクの管理には、人、プロセス、IT システムの連携が必要です。組織のあらゆるレベルで意識を醸成すること、それがサイバーセキュリティ管理を実施する際の重要な第一歩です。

KPMG[1]、EY[2]、Risk.net[3]をはじめとする経営コンサルタントの多くが、サイバー侵犯をオペレーショナルリスクの最上位に位置付けています。プリマス大学からは、船舶のオペレーターに対して旧式のシステムの脆弱性を指摘する論文が発行されています[4]。 また、複数の法律事務所が海運業を狙ったサイバー犯罪[5]の増加に警鐘を鳴らしています。急速に進化する技術を悪用する犯罪者にとって、対策が不十分なシステムにアクセスすることはたやすいことです。陸上施設との頻繁な通信、クラウドコンピューティングの利用機会の増加、コンピューターのネットワーク化、BYOD（私物デバイスの業務利用）の浸透、ソーシャルメディアや IoT の活発な利用――これらすべてがリスクの増大に寄与しているのです。

海事業界で発生しやすいサイバー攻撃の種類

これまでにも、海事業界では、サイバーセキュリティに関する様々な事案が発生しています。

- なりすましメール(Email spoofing)を利用して不正送金させた。
- GPS 信号の受信妨害による航路逸脱が発生した。
- 浮体式石油プラットフォームが片舷に傾いた（その結果、一時操業停止に追い込まれた）。
- 港のサイバーシステムに侵入して違法薬物が積載されたコンテナを探し当てて奪った。
- 海運会社のコンピューターシステムに侵入し、船内のセキュリティが手薄で、高価な積荷を積載している船を特定した上でハイジャックした。

海運業に対するサイバー攻撃の影響は?

2015 年に、ロイズは、サイバー攻撃による損害額が毎年 4 千億米ドルにのぼると試算しました[6]。また、サイバー攻撃の影響は、財務上の損失に留まりません。

- 船舶の物的損害
- 船員の身体への危険
- 積荷の損失
- 汚濁
- 風評被害
- 業務の中断

---

[1] 「KPMG Internal Audit: Top 10 key risks in 2015」
[2] 「Risk Management for wealth and assset management: EY EMEIA survey 2014」
[3] Mark Pengelly「Cyber is biggest operational risk fear, say practitioners」, Risk.net, 19 January 2016
[4] Mr. Alan Williams 「Outdated systems placing maritime vessels at risk of cyber-attack, study suggets」, Plymouth University, 24 May 2016
[5] 「Marine Cyber Fraud Alert」, Weightmans LLP, September 2016
[6] Stephen Gandel「Lloyd's CEO: Cyber attacks cost companies $400 billion every year」, Fortune, 23 January 2015

サイバーリスクに対する取り組み

デジタル化の進展に伴い、複数機関による協調的な取り組みが見られるようになりつつあります。:

- 各国当局が戦略を策定し、報告書を作成（米国、EU[7]）
- 海運関連の各種機関がサイバーセキュリティに関するガイドラインと勧告を発表（BIMCO、IMO[8]、DNV GL[9]）
- 石油・天然ガス業界は、サイバー脅威に対する共同での取り組みを行っている[10]。
- 英国の運輸省と海事沿岸警備庁が「Code of Practice on Cyber Security for Ports and Port Systems（港湾および港湾システムのサイバーセキュリティに関する実施要綱）」を作成

どこから取り組むべきか

サイバー脅威に対して最も脆弱なのは「人」です。サイバー攻撃のほとんどは、ヒューマンエラーに依拠しています。DNV GL によると、サイバー攻撃の 97 パーセントは、人の誤認を誘って重要な情報を入手しようとするタイプのものです（ソーシャルエンジニアリング[Social engineering]という）。Gard では、メンバーの皆様の利益の保護に精力的に取り組んでおり、その一環として、Gard が保有する情報を秘密漏洩、改ざん、不正アクセスから守るための、人、プロセス、IT システム面を包括した情報セキュリティ管理システム(Information security management)取得を策定中です。また、国際サイバーセキュリティ月間である今年 10 月には、サイバー攻撃のリスクとその防止への意識向上を図るための様々な活動を実施いたしました。

同様に、メンバーの皆様においても、サイバーセキュリティに対する啓蒙に取り組まれることを提案いたします。さらに詳しい情報を gard.no の「Cyber security」の特集に掲載していますので（英文）、取り組みの際の参考としてください。

---

[7] こちらをご参照ください。

[8] MSC.1/Circ.1526「Interim Guidelines on Maritime Cyber Risk Management」, IMO, 1 June 2016

[9] DNVGL-RP-0496「Cyber security resilience management for ships and mobile offshore units in operation」, DNV GL, September 2016

[10] Astrid Folkvord Janbu「Oil and gas industry joins forces in fight against cybercrime」, DNV GL, 29 September 2016