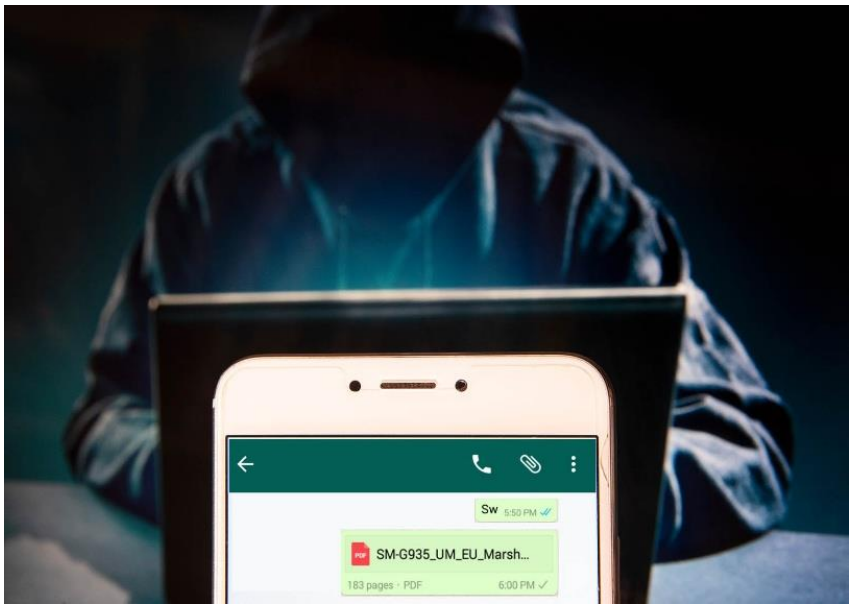
海運業界がサイバー犯罪者の標的となっています

こちらは、英文記事「Maritime industry targeted by cyber criminals」（2019 年 8 月 22 日付）の和訳です。

ノルウェー当局の調査によると、海運業界と石油・ガス業界が最近のサイバー犯罪の標的となっており、特に米国、ヨーロッパ、中東の企業が集中的に被害を受けていることが報告されています。これを受けて、ノルウェー当局は、繰り返されるサイバー活動に短中期的に備えるよう各企業に忠告しています。



ノルウェーの国家安全保障当局（NSM）は、海運業界へ向けた最近の information letter の中で、2019 年 6 月以降、あらゆる業界を標的としたサイバー犯罪が増加していることを指摘し、その中でも特に、海運業界と石油・ガス業界が攻撃の標的にされていると報告しています。

これまでに、電子メールやソーシャルメディア（LinkedIn のほか、WhatsApp や Facebook Messenger など）の個人メッセージを利用したソーシャルエンジニアリング攻撃が報告されています。こうしたソーシャルエンジニアリングの主な狙いとしては、次のものがあります。

- ユーザーのコンピューターにマルウェアをインストールする。
- ユーザー、その雇用主、またはそれらとつながっている他のユーザーに関する情報を収集する。
- サイバー攻撃を拡散する。

このようなサイバーインシデントは、世界規模で繰り返し報告されており、NSM は*「特に米国、ヨーロッパ、中東の企業が標的となっている」*と伝えています。また、こうしたサイバー攻撃者は、犯罪遂行のための高い能力を保持していることが確認されています。

NMS は、現在の状況と検出されたリスクに基づき、悪意のあるサイバー活動の企てに対して、短中期的に備えるよう企業や組織に忠告しています。また、このことは、攻撃対象になりやすい企業のみならずそれ以外の企業も被害に遭う可能性があると伝えています。つまり、船舶だけではなく、船主の陸上インフラもサイバーインシデントにさらされる可能性があるということです。さらに、

statement of 19 August 2019（2019 年 8 月 19 日発表の声明文）の中で、ノルウェー海事局（NMA）は次のように強調しています。*「特に、ISPS コードの保安レベル 2 以上の海域を運航する船主は、サイバー攻撃の現状について認識すべきです」*

推奨事項

NSM の information letter は、ノルウェーの企業に向けて発表されたものですが、船舶運航者と船内インフラの整備・運用担当企業は、デジタルセキュリティを継続的に監視・レビューするとともに、以下の推奨事項に従うようにしてください。

- ネットワークがセグメント化されているか確認すること。ネットワークの管理部分と運用部分が物理的に接続されていないようにすべきである。
- すべてのエンドポイントとネットワーク内のアクティビティを記録すること。NSM は、ログを最低 6 か月間保存することを推奨している。
- 可能な限り、船舶と陸上インフラ間でも暗号化通信を採用すること。暗号化されていなければ、通信内容が容易に改ざんされる恐れがある。
- 個人の立場や役割に応じて、情報とシステムへのアクセスを制限すること。大抵の場合は、アクセスの制限により、インシデント発生後の被害を抑えることができる。

NSM は、推奨される対策の中でも特に、サイバーセキュリティ意識向上訓練の重要性について強調しています。船員、陸上スタッフ、その他の関係者を含むすべての「ユーザー」は、以下について留意してください。

- 添付ファイルやリンクを含むメールに注意・警戒すること。
  - 添付ファイルやリンクの安全性が疑われる場合は、それらを開く必要があるかどうかよく考える。会社に関連する不審な電子メールやメッセージを受信した場合は、雇用主に報告する。
  - Word、Excel、PowerPoint のマクロの有効化を促す警告メッセージには注意する。
- ソーシャルメディアでは以下の点に注意すること。
  - ソーシャルメディアを介して不審なメッセージを受信した場合は報告すること。特に、メッセージが業務や会社全般に関連したものである場合。
  - 本人確認ができる相手とだけコンタクトを取ること。
  - リンクや添付ファイルを含まれたソーシャルメディアのメッセージには十分に注意すること。この手の攻撃が増加している。
  - ソーシャルメディアで共有した情報（仕事や私生活に関するものすべて）は、誰もがアクセス可能であることに留意する。
  - 雇用主の同意なしに、ソーシャルメディアで仕事関連の情報を公開しないこと。
  - 同意なしに他者に関する情報を公開しないこと。

- 製品やアプリケーションで利用可能なセキュリティ設定を有効にする。
- 複数のサービスで同じパスワードの使い回しをしないこと。
- サイバー攻撃が疑われる場合、また、対処方法が分からない場合は、セキュリティの **STAR**「**S**top – **T**hink – **A**sk – **R**eport」（冷静になる、考える、他の人に聞く、報告する）を徹底すること。

船舶運航者は、自国の国家安全保障当局によるサイバーセキュリティに関する忠告にも細心の注意を払う必要があります。例えば、ノルウェー企業は、NSM による「Fundamental principles for information and communications technology (ICT) security（情報通信技術セキュリティに関する基本方針）」および「Measures and recommendations concerning social media（ソーシャルメディアに関する対策と推奨事項）」に従うよう推奨されています（いずれもノルウェー語版のみ）。また、船舶運航者と船員は、不審な活動やセキュリティ侵害行為のすべてを、旗国の当局や国家安全保障当局に報告してください。報告することで、進行中のサイバー攻撃の脅威とリスクの監視が強化されます。

その他のガイダンス

サイバーリスク管理に関するその他の推奨事項について、Alert 記事「これ以上、サイバーセキュリティを見過ごすことはできません」（2019 年 7 月 10 日付）および「船上のサイバーセキュリティ管理を強化すべき時期です」（2018 年 12 月 12 日付）を参照してください。また、Gard と DNVGL が共同で作成したロスプリベンション意識向上ビデオ（英語）が、啓蒙活動を実施する上で役立つと思われます。

船舶運航者は、2021 年 1 月 1 日以降に実施される ISM に関する初回の年次監査までに、船舶の既存の安全管理システムが、ISM コードで定義されている基準を満たし、サイバーリスクに適切に対処できるようにしておく必要があります。サイバーリスク管理を実装するためのガイドラインとベストプラクティスについては、IMO による「MSC-FAL.1/Circ.3（海上サイバーリスク管理のガイドライン）」や、海運業界のガイドライン「Cyber security onboard ships（船上のサイバーセキュリティ）」をご覧ください。