デンマークが海運セクターのサイバー脅威を確認

こちらは、英文記事「Denmark identifies cyber threats in its maritime sector」（2019 年 1 月 24 日付）の和訳です。

デンマーク当局は、海運セクターに対する一般的なサイバー脅威は主として商取引に向けられたものだと結論付けましたが、その一方で、脅威は絶えず変化しており急変する場合があるという点についても強調しています。

2018 年 12 月の Gard Insight「It is time to strengthen your onboard cyber security procedures（船舶のサイバーセキュリティに対応する手続きを強化すべき段階）」に関連して、デンマークの商務・金融省はこのほど、「Cyber and Information Security Strategy for the Maritime Sector（海運セクターのサイバー・情報セキュリティ戦略）」を策定しました。この戦略はデンマーク政府のサイバー・情報セキュリティに係る国家戦略の一部ですが、デンマークの海運セクターにおける脅威やリスク、脆弱性に関連する興味深い所見が示されています。

この戦略の対象はデンマークが主体ですが、デンマーク国外の標的を狙ったサイバー攻撃についても取り上げています。デンマークのいくつかの海運会社はグローバルに展開しており、デンマーク籍船舶とその船員は海外で運航や商業活動を行うことが多くなっています。したがってサイバーリスク管

© 2019 Gard AS

理を自社の安全管理システム（SMS）に組み入れる際には、デンマーク以外の海運会社も、この戦略の以下の主要なメッセージをぜひ確認しておくといいでしょう。

脅威の評価

デンマーク政府が策定した戦略では、海運セクターに対する一般的な脅威は商取引に向けられているものであり、現在は海上での活動には直接脅威を与えていないと結論付けています。戦略では、デンマークサイバーセキュリティセンター（CFCS）による 2019 年 1 月の 脅威の評価（英文）に基づき、以下の点について考察を行っています。

- **サイバースパイ**の脅威は**非常に高い**。民間企業や公共機関へのサイバースパイ活動に対して外国が経済的にも政治的にも関心を持つ可能性がある。
- **サイバー犯罪者**の脅威は**非常に高い**。サイバー犯罪者は海運セクターの民間企業や公共機関を標的にさまざまな種類のサイバー攻撃を行う。サイバー犯罪によって経済的影響に加えて、最悪の場合、海運セクターの操業が途絶する可能性がある。
- **サイバーアクティビズム**の脅威は**低い**。サイバーアクティビストは、通常、イデオロギー的または政治的理念を動機としており、その理念に反するとアクティビストがみなす個人または団体が標的となる。問題となっている物品の輸送または船舶からの石油流出など、海運セクターが関係する政治的事象や事件をきっかけにハッカーが素早く動員されるため、脅威は突然高まる可能性がある。
- **サイバーテロ**の脅威は**低い**。少数の軍の過激派がサイバーテロを行うことに関心を示しても、現在はそれを実行する能力がない

ただし、注意すべき点は、この評価は、脅威を取り巻く現在の状況に基づき、0〜2 年の期間を対象に実施しており、また、サイバー脅威は、海賊行為などの他の海上の脅威と同様に常に変化しているため、急激に変わる可能性があるということです。海運業や船舶、船員を攻撃しようとする犯罪者は、よく組織化され独自のやり方で進化し続けていますが、これは常に進化を続けるサイバーリスクの全般的な性質を示しています。

リスクと脆弱性の分析

新たに刊行された「Industry cyber risk management guidelines（産業サイバーリスク管理のガイドライン）」第 3 版に記されているとおり、デンマークの戦略は、船舶の情報技術（IT）と運用・制御技術（OT）システムの統合と互換性に関連する問題が大きなリスクであると考えています。
OT システムに関連するリスクは、IT システムに関連するリスクとは異なります。IT システムの不具合によって船舶の荷降ろし、または通関に大幅な遅延が生じる可能性がある一方、OT システムの混乱は船員や貨物の安全に大きなリスクをもたらし、海の環境に損害を与え、船舶の運航に支障を与える可能性があります。戦略では、この二つのシステムに「技術の差」がある可能性があること、（OT の不具合が深刻な結果を招くおそれがあるにもかかわらず）船会社は OT システムのメンテナ

© 2019 Gard AS

ンスやアップグレードが手薄になりがちであることを強調しています。また、OT システムのアップグレード手順が IT システムのガイドラインに適合するとは限らない点についても指摘しています。

推奨事項

この国家戦略では、デンマーク海事局（DMA）が実施予定のいくつかの積極的な取り組みが示されているほか、以下の項目の重要性を強調しています。

- サイバーリスク管理手順策定の際には、関連する国際基準、産業標準、ベストプラクティスを確認するとともに、管理対策が各企業固有のリスクプロファイルに適合していることを確認する
- サイバーセキュリティに対する意識向上を図る。サイバーセキュリティで現在鎖の最も弱いつなぎ目（最も脆弱な部分）はヒューマンファクター（人間がエラーを引き起こすこと）です。
- サイバーセキュリティに関するコミュニケーション、管理、指導は、必ずトップマネジメントからの指示で行うようにしてください。サイバーセキュリティに関しては、船舶や部門ごとに個別に対処すべきではありません。
- サプライヤーのセキュリティレベルおよびサプライヤーのセキュリティ品質性能の確認については、個別に要件を定めてください。

その他の推奨事項については、2018 年 12 月の Gard Insight「It is time to strengthen your onboard cyber security procedures（船舶のサイバーセキュリティに対応する手続きを強化すべき段階）」を参照してください。

DNVGL と Gard が共同制作した情報漏洩対策意識向上ビデオ（英語）もご覧ください。

本情報は一般的な情報提供のみを目的としています。発行時において提供する情報の正確性および品質の保証には細心の注意を払っていますが、Gard は本情報に依拠することによって生じるいかなる種類の損失または損害に対して一切の責任を負いません。

本情報は日本のメンバー、クライアントおよびその他の利害関係者に対するサービスの一環として、ガードジャパン株式会社により英文から和文に翻訳されております。翻訳の正確性については十分な注意をしておりますが、翻訳された和文は参考上のものであり、すべての点において原文である英文の完全な翻訳であることを証するものではありません。したがって、ガードジャパン株式会社は、原文との内容の不一致については、一切責任を負いません。翻訳文についてご不明な点などありましたらガードジャパン株式会社までご連絡ください。

© 2019 Gard AS