海事インフラのサイバーセキュリティ

Cyber security of maritime infrastructure

島田裕樹・ネットワーク分科会・情報セキュリティ大学院大学

〈Abstract〉

There are many cases of well-known cyber attacks occurred on shore, but cases of cyber attacks related to maritime also occurred. However, as no cases have become major topics in the country yet, it is considered that the domestic popularity of cases of cyber attacks related to maritime is low. At least domestically, few have concerns about cyber security of maritime infrastructure. In this paper, based mainly on overseas literature, author investigated trends in cyber security of domestic and overseas maritime infrastructure and describe about investigated the laws, guidelines, vulnerabilities of systems and equipment, and cases of actual cyber attacks. Based on the found out content, we will examine the motivation of attackers to attack vessels and ports constituting the maritime infrastructure and the attack scenarios that may occur in the future.

海外では船舶や港湾で使用されているシステムについて脆弱性が指摘されている。

GPS

船舶に対するGPSジャミングの実験やGPSスプーフィングの実験が報告されており、どちらも成功している。

ICS（産業用制御システム）

海事関係では船舶の内部や貨物移動などで使用されている。比較的最近のICSはネットワーク接続されるようになった一方で機密性や完全性よりも可用性が優先されるためセキュリティ向上が困難であることなどを指摘されている。

ECDIS（電子海図表示システム）

デモ製品について、古いバージョンのApache Web serverがローカルで実行されていたことによるセキュリティ上の脆弱性を明らかにしたとする報告がなされている。

AIS（船舶自動識別装置）

トレンドマイクロ社からセキュリティ評価を行った資料が公開されており、AISを悪用することによる様々な脅威が指摘されている。

VDR（航海情報記録装置）

海外で古野電気株式会社製のVR-3000に関する脆弱性が報告され、JVNからも同製品に関する脆弱性が公表された。

衛星通信で使用される様々な装置

複数のバックドア、ハードコードされた資格情報、文書化されていないプロトコル、弱い暗号化アルゴリズムなどの脆弱性が発見された

海外では実際に海事関連のサイバー攻撃が発生している。

ベルギーのAntwerp港における事例

薬物を密輸する目的で、密売グループがハッカーを雇ってコンテナターミナル事業者や港湾会社のコンピュータに不正に侵入していた。

メキシコ湾の移動式海洋掘削装置が操業停止に陥った事例

労働者がスマートフォンやその他の個人的な機器を掘削装置のナビゲーション制御システムに接続し、その際に感染したマルウェアによって現場が一時的に中断した。

主に日本と韓国を対象とした標的型攻撃

Icefogと呼ばれるマルウェアを用いた標的型攻撃の事例では、攻撃者は様々な分野の企業などに関心を持っていたとされるが、その中には造船会社も含まれている。

イランの船会社IRISLに対する攻撃

攻撃により料金、貨物重量、貨物番号、日付、そして、場所に関連する全てのデータに損害が与えられ、コンテナの所在が誰も分からない状態に陥った。

海賊が船舶から特定のコンテナの中身だけ奪った事例

海賊が事前に船会社が自社開発したCMSを攻撃して、目的のコンテナと、それを輸送する船舶を特定していた。

金銭の窃取

船舶の燃料費などを通常とは別の口座に振り込むように求める詐欺メールの事案や、攻撃者が業者のメールアカウントをハッキングして船会社に支払いを要求した事案などがある。

韓国へのGPSジャミング攻撃

北朝鮮によるものと思われる攻撃が2010年以降に度々発生し、その度に船舶の航行に影響を与えている。

オーストラリア税関国境警備局の貨物システム侵入

犯罪組織が貨物システムに侵入することで警察や税関当局がどのコンテナを疑わしく考えているのかチェックして、その情報をもとに密輸コンテナを放棄していた。

VDRのデータ破壊

船舶が他の漁船と衝突した際にVDR（航空機でいうところのブラックボックス）のデータが改ざんされた可能性のある事案がある。

攻撃者の動機と、陸上でのサイバー攻撃との違い

海事関連のサイバー攻撃において、攻撃者の動機は「物品」「金銭」「情報」「妨害」に大別される。

	物品	金銭	情報	妨害
海上	主に薬物の密輸やコンテナ内の貴重品など、その物品を得ること自体が攻撃の目的となっているケースが存在する。	船会社に対して関係者を装い、船舶の航行に必要な金銭を攻撃者の口座に振り込むように電子メールで連絡し、巨額の金銭を騙し取る手口が存在する。	サイバー攻撃で船会社から窃取した輸送船舶や積荷の詳細などに関する情報を、コンテナの窃盗や海賊行為などに利用するケースがある。	陸上と同じく、船会社に対するサイバー攻撃によるデータの削除が挙げられるが、GPSジャミングによる船舶の航行妨害も挙げられる。
陸上	目立つ事例は見当たらない。	例としてランサムウェアによる攻撃が挙げられる。	例として標的型攻撃が挙げられる。	例としてStuxnetによる事案やDDoS攻撃、サイバー攻撃による組織内のデータの削除が挙げられる。