自動運航船のサイバーセキュリティ対策の提案

A Proposal for Cybersecurity Measures for MASS

二神豪・ネットワーク分科会・情報セキュリティ大学院大学

1. 研究背景

近年、衛星通信技術等の発展に伴い、海上の通信環境が改善され、メールやインターネットでの情報収集が中心だったシステムの利用目的が運航管理等のために船舶のOT系データを陸上と情報連携するなど、変化が見られる。ただ、現在の一般的な船舶においては、外部ネットワークから船舶のシステムに侵入し、機関や操舵の乗っ取りが可能な段階には至っておらず、サイバーセキュリティリスクは顕在化していない。一方、現在研究開発が進められている自動運航船には遠隔操船機能など、様々な機能が必要となることから、自動運航船が実用化された場合、IT/OTシステムがインターネット環境にさらされることになり、サイバーセキュリティリスクが増大することが予想される。

2. 目的

船舶がフィジカルの世界で引き起こす事故は、人命・財産・環境等に深刻な被害をもたらす可能性が高く、自動運航船のサイバーセキュリティ対策についてはライフサイクルを通して万全を期す必要があるため、そのあり方について検討し、提案を行う。

3. これまでの調査結果

先行して自動化が進められている自動車・工場のシステムと比較し、自動運航船の課題について以下のとおり判明した。

- ✓ 船舶には、他船識別装置（AIS）、電子海図表示装置（ECDIS）、航海データ記録装置（VDR）及びOT系通信規格（NMEA）といった固有の装置・プロトコルが採用され、将来の船舶の自動化に向けた課題（脆弱性）がある。
- ✓ 船舶は、受注生産で一品一様であり、設計段階において、コスト削減のため無駄な空間がないように設計されており、不具合のある装置を新しく更新することは困難である。
- ✓ 船舶の寿命は、20年～30年と長い。
- ✓ 船舶の法定の乗組員にIT/OTの専門家はいない。
- ✓ 船舶は修理する場合は遠隔地にあるドックに入渠する必要があり、自動車のように手軽にディーラーに持ち込むことはできないため、頻繁にメンテナンスを行うことは困難である。

4. 今後取り組むべき課題

自動運航船のライフサイクルを通したセキュリティ対策の課題は以下のとおり。

- ➢ 既存装置の脆弱性対策とセキュア・バイ・デザインのあり方
- ➢ リモートメンテンナンス（OTA）のあり方
- ➢ ライフサイクルを通したメンテナンスのあり方

【今後の研究計画】

～3月頃　自動車及び工場における上記課題に対する方策を詳細に調査・比較し、検証する。
～5月頃　自動運航船固有のサイバーセキュリティリスクを明らかにし、その対策について検討し、評価する。
9月頃　中間発表　　1月頃～　修論提出、審査・最終試験、研究成果発表