

自動運航船のサイバーセキュリティ対策のための MASS-BOMの提案

Proposal of MASS-BOM for Cybersecurity Measures for Autonomous Ships

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

Modern vessels often neglect operational technology (OT) software maintenance, leaving critical vulnerabilities unaddressed. Commercializing Maritime Autonomous Surface Ships (MASS) requires resolving this to prevent unauthorized remote control. To enhance complex system transparency, this thesis proposes MASS-BOM, a framework for centrally managing and sharing system configuration information across the maritime industry. We analyze its core components and lifecycle, discussing practical applications for OT maintenance. Furthermore, by applying actual vessel failure incidents as case studies, we evaluate MASS-BOM's effectiveness. The findings demonstrate its significant potential to facilitate secure OT software maintenance and resolve critical operational challenges in the maritime sector.

1. 研究背景と目的

船舶では、他のシステムへの影響・可用性を考慮し、OT系ソフトウェア・メンテナンスが実施されておらず、脆弱性が放置されており、中には、既に悪用され、深刻な被害を及ぼした脆弱性の残存も確認されて

OT系ソフトウェア・メンテナンスにおける障害事例

- 出港後間もなく、統合ナビゲーションブリッジシステムがほぼ全停止
- 出港地において、メーカー技術担当者により、航海用ソフトウェアをアップデートしたところ、ECDIS(電子海図装置)のOSが旧式(非対応)であり、航海用ソフトウェアを起動できなかった。
- 紙海図等により航行を継続し、後日、新しいECDIS装置の搭載、船級検査等が必要となり、費用は船主が負担した。

影響評価が不十分

IT技術者不足

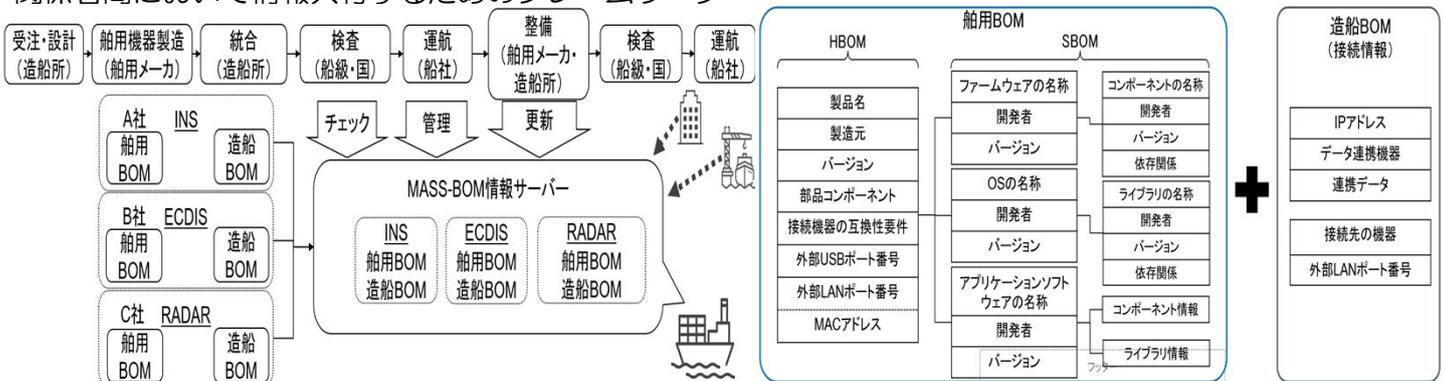
システム構成
情報の困難性

システム依存
関係のブラック
ボックス化

IT技術者不足

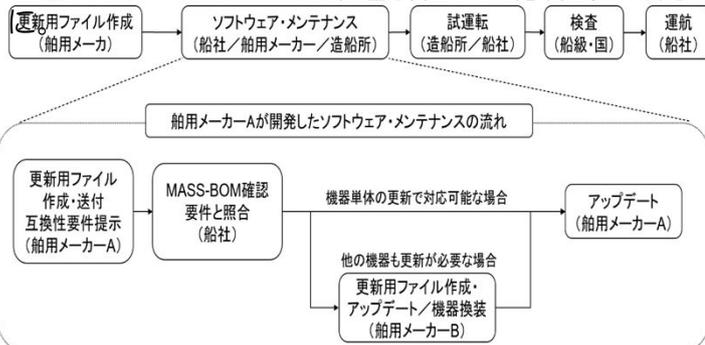
2. 船舶のシステム構成情報の管理・共有フレームワーク (MASS-BOM)の提案

MASS-BOMは、船舶のシステム構成情報を包括的かつ一元的にライフサイクルを通して集約・管理し、関係者間において情報共有するためのフレームワーク



3. ソフトウェア更新への活用

MASS-BOMにより船社が主体的にOT系ソフトウェア・メンテナンスの影響評価・実施判断が可能



4. ケーススタディを用いた考察・検討

船舶で実際に発生した障害事例をケーススタディに適用し、MASS-BOMの有効性を考察・検討

- システム構成情報の把握が容易となる見込み
- 依存関係・接続関係が可視化される見込み
- 乗組員でなくてもOT系ソフトウェア・メンテナンス及び脆弱性管理の実施判断が可能となる見込み

5. 今後の展望

本研究はMASS-BOMの概念レベルであり、実装には至っていないことから、引き続き、船舶のシステム構成等の実態を調査し、実装及び評価検証に向けた取組を継続する所存。