本プレスリリースは関係社より同日に配信いたします。

株式会社ＮＴＴデータ
株式会社 MTI
ジャパン マリンユナイテッド株式会社
一般財団法人 日本海事協会
日本郵船株式会社
（法人名は五十音順）

2020 年 7 月 20 日
2020-015

国内初、船上機器システムへのサイバー攻撃を想定した検証の実施及び検証成果の公開

株式会社ＮＴＴデータ、株式会社 MTI、ジャパン マリンユナイテッド株式会社、一般財団法人日本海事協会、日本郵船株式会社は、既存船舶の船上機器システムを模擬した環境において、船舶へのサイバー攻撃を想定した「ペネトレーションテスト（侵入テスト）」(*1)を国内で初めて実施しました。また、船上機器システムに関わるサイバーリスク対策の検証手法の確立を目指す取り組みとして、その成果を一部公開しました。

【背景】

IT (Information Technology)の発達に伴い、船舶においても、船内機器の電子化や、船陸間の衛星通信の普及が進んでいます。その一方で、第三者による船舶システムへの不正アクセスなど、サイバーセキュリティ上のリスクが世界的にも高まっています。これらの不正アクセスにより、エンジンの異常運転や停止を引き起こしたり、航海計器の表示や位置情報を改ざんする事で、意図的に操船を乗っ取るといった脅威が指摘されています。

上記のような背景から、船舶運航におけるサイバーリスク管理については、国際海事機関（IMO）において、2021 年以降に安全管理システムの中で対応することを推奨する国際ガイドラインが採択されました。また船舶・船上機器システムのセキュリティ対策においても、国際船級協会連合(IACS)の統一規則や、各船級のガイドラインで要求されています。しかしながら、船上機器システムへの機能要件の検討が進む一方で、実装されたサイバーリスク対策がこれらの要件を満たすことを検証する手法は、確立の途上にあります。

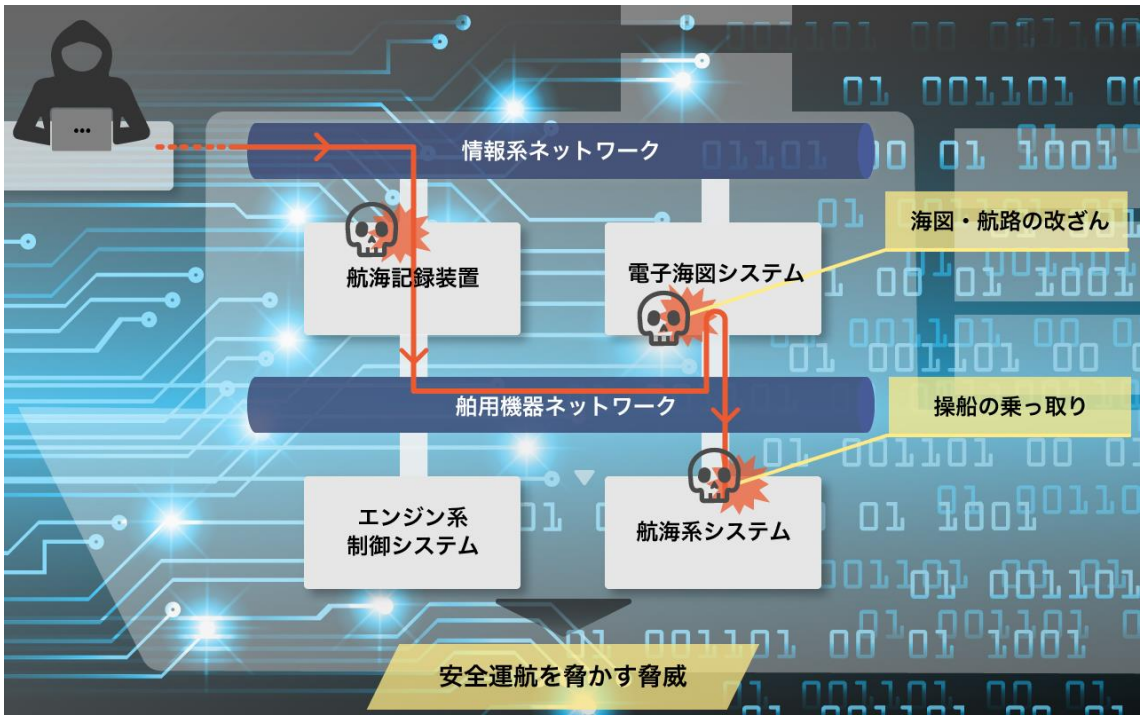
【ペネトレーションテストの実施と成果】

前述のような背景を踏まえ、上記5社は、サイバーリスク対策の検証手法として、既に他産業で活用されているペネトレーションテストの有効性の確認及び知見を獲得するべく、船社、造船・舶用事業者といった業界関係者とIT業界が手を組み、新造船を想定した模擬環境において、同テストを実施しました。その結果、船上機器が攻撃を受けた後の本船上での対応や、テスト結果に基づく事前対策のルール形成が必要と評価されました。

そして、ペネトレーションテストの成果は、適切なサイバーリスク対策の検証手法の確立、及び日本の海事クラスターのサイバーセキュリティに関わる技術水準向上の一助となるよう、一部を「船上機器システムにおけるサイバーリスク対策検討のためのペネトレーションテスト成果報告書」として公開しました。

本報告書ではペネトレーションテストの体制や手順、実施上の留意点など、本テストのユーザが今後テストを実施・運営していくにあたり参考となる情報のほか、テスト結果から得られた船上機器システムにおけるサイバー攻撃対策として有用な事例についても紹介し、船社、造船・舶用事業者のサイバー攻撃への備えに貢献することを目指します。

報告書URL: https://www.classnk.or.jp/hp/pdf/press/report/202007j.pdf



【今後の展望】
船舶の安全運航のためのサイバーセキュリティ対策においては、船舶運航者、造船事業者、船級協会を始めとする、海事業界の様々なプレイヤーが、サイバーセキュリティ対策に強みを持つ IT 企業とも協力しながら、迅速かつ強固に連携して対応していくことが、今後求められていきます。
今回の取り組みを通じて、海事クラスターがより連携し、海事産業全体の安全性向上にも寄与することを目指しています。また、実際のインシデント発生後の対応や、船内システム相互のネットワークを含めたテストを行い、必要となる対策立案に役立てます。

(*1)ネットワークや当該ネットワーク上に存在する情報端末やサーバといったノードに対し、ホワイトハッカーが疑似的なサイバー攻撃を実施することで、攻撃主体が披験ネットワーク上の情報資源に対してどのような行為を成し遂げうるかということを明らかにするテスト。

(*2)ノード：コンピュータネットワークを構成する機器それぞれの事

【本プロジェクトにおける各社の役割と取り組み】
■株式会社 NTT データ
NTT データの侵入テストノウハウが船上機器システムのサイバー攻撃耐性検証へ活かせること、NTT の先進技術がサイバー攻撃検知に有効であることを確認しました。NTT データは OA システムのみならず、工場、電力施設、化学プラント、港湾施設といった重要インフラなどの制御系システムを対象とした侵入テストサービスを展開します。

■株式会社 MTI
船舶のハードウェアとソフトウェアに関わる技術的知見を活かし、本プロジェクトの企画運営に携わりました。自律船に代表される、今後の船舶への高度自動化システムの搭載においても、今回のプロジェクトの成果を活かして、国内外の多くのプレイヤーと連携して、安全な船舶の実現を目指していきます。

■ジャパン マリンユナイテッド株式会社
今回、対象機器選定やシナリオ構築に携わることによって当事者として必要な多くの知見を得ることができたと同時に、自社建造船において実際にどのようなリスクが存在するのか初めて明らかにすることができました。
サイバーリスク対策は各企業単独でなく業界全体での対応を求められており、当社としても引き続きあるべき新造船の姿の構築に向けて検討を続けてまいります。

■一般財団法人日本海事協会

第三者機関である船級協会として、船舶のサイバーセキュリティ確保のために各ステークホルダに求められる役割・要求事項を整理しました。本プロジェクトにより得られた知見を、「ClassNK サイバーセキュリティアプローチ」の考え方に基づいて、本会のガイドライン策定に活用するなど、海事産業に還元してまいります。

■日本郵船株式会社

船会社としての安全な航海を維持するという視点から、本プロジェクトにおける、ペネトレーションテストの実施シナリオ考案に参加しました。今回の知見を活かし、世界の物流とライフラインを支える企業として、より安全で安定的な船舶運航と物流の実現に努めていきます。

本件に関わるメディアお問い合わせ先：

株式会社ＮＴＴデータ	広報部	050-3644-3022
株式会社 MTI	広報担当	info@monohakobi.com
ジャパン マリンユナイテッド株式会社	総務部 広報グループ	045-264-7200 contact@jmuc.co.jp
一般財団法人日本海事協会	広報室	03-5226-2047 eod@classnk.or.jp
日本郵船株式会社	広報グループ　報道チーム	03-3284-5178