July 2020

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

2020 年 7 月

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

改訂履歴

No.	日付	区分	改訂内容
1	2020.7.20	新規	新規作成

目次

1　背景と目的 1
1.1　背景 1
1.2　本プロジェクトの位置づけ 1
1.3　目的 2
2　ペネトレーションテスト 2
2.1　ペネトレーションテストの意義 2
2.2　ペネトレーションテストの実施体制と手順，レッドチームの動作 4
2.2.1　実施体制 4
2.2.2　実施手順 6
2.2.3　レッドチームの動作 6
3　オンボードシステムへのペネトレーションテストの実施 8
3.1　実施概要 8
3.1.1　実施体制 8
3.1.2　被験システムの選定 8
3.1.3　レッドチームの攻撃手法と勝利の定義 10
3.1.4　本テストにおけるレッドチームのアクションに関する前提と制約 11
3.1.5　攻撃シナリオの設計要件 11
3.1.6　被験システム主管の負担 12
3.1.7　実施スケジュール 12
3.2　航海機器系システム試験内容 13
3.2.1　実施期間および実施環境 13
3.2.2　攻撃シナリオと攻撃の勝利条件 13
3.3　機関系システム試験内容 15
3.3.1　実施期間及び実施環境 15
3.3.2　攻撃シナリオと攻撃の勝利条件 15
4　まとめと考察 17
4.1　PTの効果 17
4.1.1　オンボードシステムに対するレッドチームの攻撃行動 17
4.1.2　レッドチームの攻撃行動への対策例 18
4.1.3　今後の検討が必要な事項とその対応例 19
4.2　PT実施体制・手順などの知見 22
4.3　PT実施要件として今後検討すべき事項 22
4.3.1　今後の検討が必要な項目の全体像 22
4.3.2　PT実施タイミングの検討と今後のアクション 23
APPENDIX IoTセキュリティオーケストレーションエンジンの検証 26
A.1 背景と目的 26
A.2 ISEの概要 27
A.3 技術検証における前提・制約 28
A.4 古野電気実験環境における評価の概要 28
A.5 日本無線実験環境における評価の概要 30
A.6 Future work 32

略語表

略語	綴り
AIS	Automatic Identification System
BIMCO	Baltic and International Maritime Council
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
ECDIS	Electronic Chart Display and Information System
GPS	Global Positioning System
GUI	Graphical User Interface
IACS	International Association of Classification Societies
IMO	International Maritime Organization
ISM コード	International Safety Management Code
MSC	Maritime Safety Committee
PCU	Process Control Unit
VDR	Voyage Data Recorder
VDU	Visual Display Unit

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

1. 背景と目的

1.1 背景

IT (Information Technology)の発達に伴い，海事分野においても，船舶機器のコンピュータ化や船内 IP ネットワークの高度化，および船陸間衛星通信の普及が進んでいる。その一方で，悪意ある第三者による船舶システムへの不正アクセスなど，航行の安全侵害や経済的損害等の様々なサイバーセキュリティ上のリスクが懸念されている。

船舶運航におけるサイバーリスク管理（Cyber Risk Management）については，2017 年の IMO MSC98 の決議に基づき，就航船においては，2021 年 1 月 1 日以降の最初の適合証書の年次検査までに，ISM コードに基づく安全管理システムを通じたサイバーリスク管理が推奨されることとなった。

一方で，船舶それ自体のサイバーセキュリティ対策においては，今後，船上の OT（Operation Technology）機器システムの脆弱性やセキュリティリスク対策について, 新造船建造時には造船事業者がシステムインテグレーターとして主体的に, Security by Design の観点からその対策をおこなうことも IACS の UR-E22 等において必要とされるようになり, 当然, 舶用機器ベンダにおいても対応が求められてくる。

Security by Design の観点で，船上機器システムに必要な「機能要件」は，各国船級協会や，国際標準化団体よって検討がすすめられ，ガイドライン策定や，標準化が議論されつつある。

しかし，それら要件の実装が十分に満たされているかを「検証」して「認証」する方法については，まだ海事業界内での議論や検証が不十分な状況であると言える。

一方で，製造業など他産業におけるサイバーセキュリティ対策に目を向けると，製造設備における脆弱性診断や機能要件の検証に，ペネトレーションテスト（以下，PT）の実施が広く浸透している状況にあり，海事業界においても，「検証」において PT を実施することが現実的であるのかを検討することが求められている。

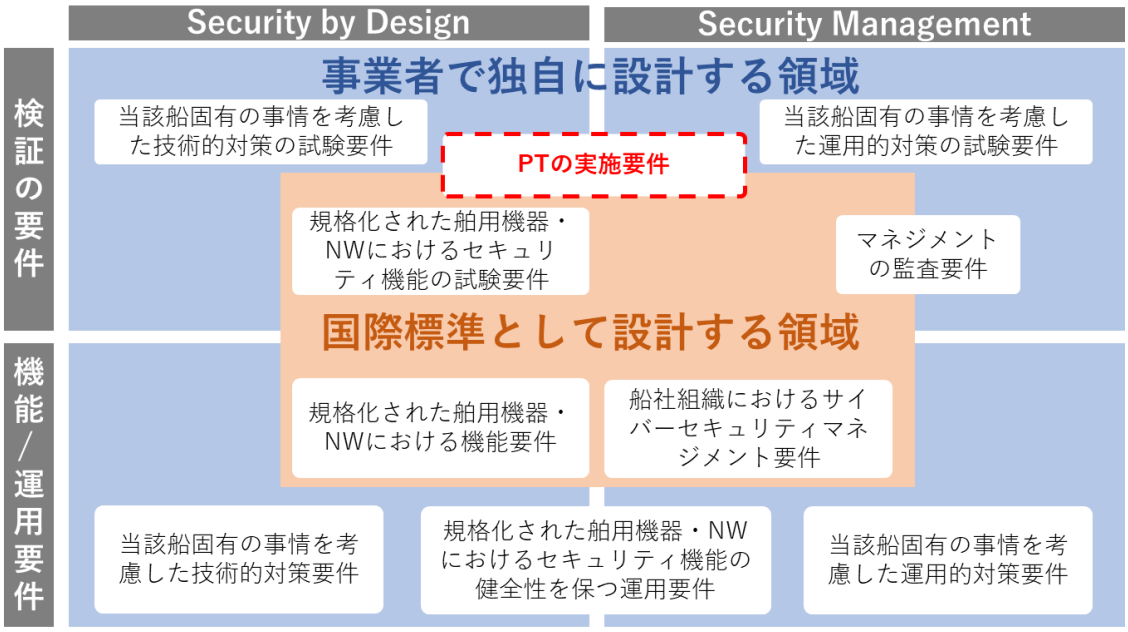


図. 1. 1. 1 海事業界におけるサイバーセキュリティの状況と PT の実施要件の位置づけ

1.2 本プロジェクトの位置づけ

前述の背景を踏まえ，船社，船級，造船事業者，舶用機器ベンダとで連携し，サイバーセキュリティの専門家として NTT データの協力を得ながら，新造船建造時に，造船事業者や舶用機器ベンダがどういう対応を今後していくべきかの検討プロジェクト（以下，本プロジェクト）を立ち上げた。具体的には，既存の船上機器・システムに対する PT プログラムを企画し実施した。

検討にあたっては，就航後の船舶運航におけるサイバーリスクの低減を念頭において，何が船舶安全運航上クリティカルなインシデントであるかを船社，船級等と一緒に議論して定義をした。本プロジェクトの参加者とその役割は表 1.2.1 の通りである。

表 1.2.1 本プロジェクトの参加者と役割

役割	企業名	業種	本報告書での略称
プロジェクト統括	ジャパン マリンユナイテッド株式会社	造船事業者	JMU
	株式会社 MTI	船社	MTI
被験機器・システム主管	寺崎電気産業株式会社	舶用機器ベンダ	寺崎電気
	東京計器株式会社		東京計器
	ナブテスコ株式会社		ナブテスコ
	日本無線株式会社		日本無線
	BEMAC 株式会社		BEMAC
	古野電気株式会社		古野電気
アドバイザリー	一般財団法人日本海事協会	船級	ClassNK
	日本郵船株式会社	船社	日本郵船
テスト運営支援	株式会社 NTT データ	IT	NTT データ
テスト実行	株式会社イエラエセキュリティ		イエラエセキュリティ

1.3 目的

本プロジェクトの直接的な目的は２つある。1 つ目は，舶用機器ベンダ，造船事業者，船社，船級といった海事産業の主要なプレーヤーが舶用機器・システムに対する PT を実際に体験し，PT の効果や実施体制・手順などの知見を獲得することである。2 つ目は，PT を船舶サイバーセキュリティ対策の運用/機能の検証手段として位置付けた場合の，実施要件として今後検討すべき項目を洗いだすことである。

また中長期的な目標として，闇雲にすべての脆弱性に対応して検証するのではなく，「守るべき対象，範囲，優先順位」を定め，造船事業者や舶用機器ベンダが余計な負担なく，適切なセキュリティ対応が可能になることを目指す。

なお，本プロジェクトでは稼働状態の舶用機器・システムに対するサイバー攻撃の発生有無を判定する攻撃検知技術についても併せて検証している。当該検知技術は舶用機器・システム間を流れる健全な通信を学習することで，サイバー攻撃起因の異常な通信を識別する技術である。現行の標準的な船舶設備において当該技術の導入は時期尚早であると思われるが，将来的な舶用機器・システムの発展に伴い，当該技術の導入を検討する段階においても当該技術の基本原理は大きく変わることはないものと予想される。そこで海事クラスターへの情報提供として本検証結果を Appendix に記載する。

2 ペネトレーションテスト

2.1 ペネトレーションテストの意義

一般的に，PT とは，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疑似的なサイバー攻撃を実施することで，攻撃主体が被験ネットワーク上の情報資源に対し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である。被験組織のビジネス固有の脅威を特定し，当該脅威の顕在化を目的とした攻撃シナリオに沿って実行される PT は，特に脅威ベースペネトレーションテスト（Threat Led Penetration Test）と呼ばれる。従来の PT は，対象となるネットワークやそのノード（以下，システム）のサイバー攻撃耐性を評価対象としているが，脅威ベースペネトレーションテスト（以下，TLPT）ではそれに加えて，サイバー攻撃を認知した際の，事業継続性の確保や被験システムの復旧に必要な組織的対処行動についても評価の対象に含むことがある。

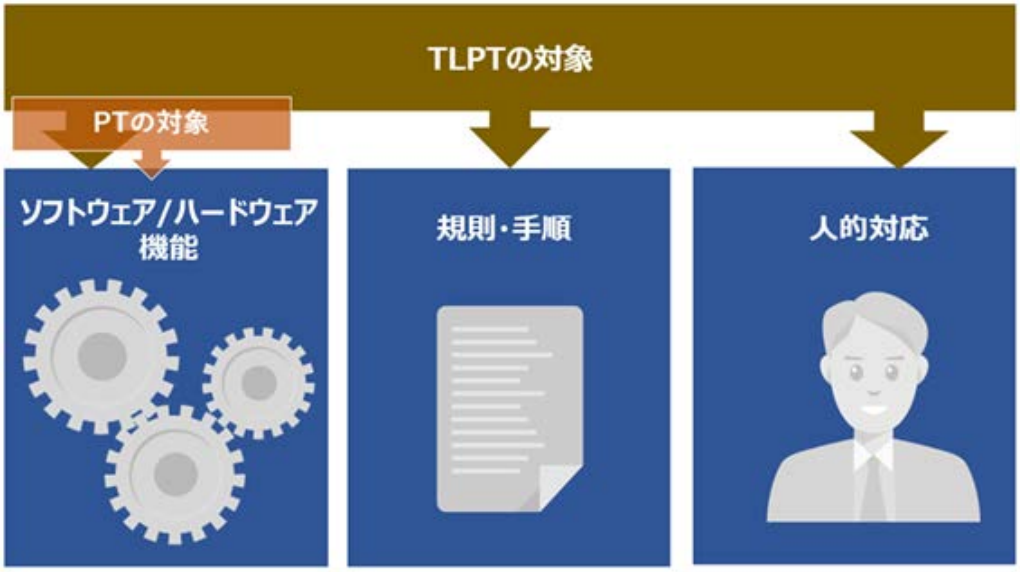
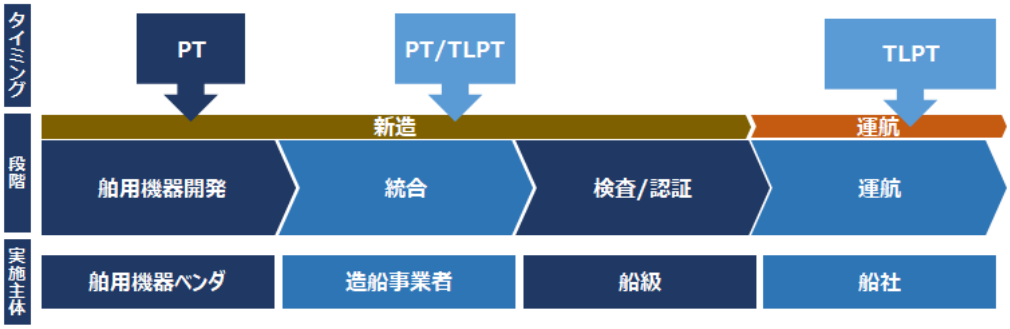


図 2.1.1　TLPT の評価対象

PT は，複数の計算資源がネットワーク化されたシステムを対象とするものであり，実施タイミングを対象システムの稼働後，あるいは稼働直前とすることがその目的に沿うものである。一方，開発工程において開発機器に対して個別に実施するセキュリティテストはソースコード診断，ファジング検査，脆弱性診断といったテストになる。

ソフトウェアプログラムやハードウェアによって船内に構築されるシステム（以下，オンボードシステム）のライフサイクルにおいて PT を実施するタイミングと実施主体については以下が想定される。

- 舶用機器群で構成されるシステムを造船事業者へ納入する前段階において，当該システムを開発した舶用機器ベンダによって PT を実施する。
- 各舶用機器ベンダより納入された機器群をインテグレートし，オンボードシステムを稼働直前状態とした段階で，造船事業者により PT/TLPT を実施する。
- 運用を開始したオンボードシステムと，当該システムの運用にかかわる組織の健全性を評価するために，船社によって定期的に TLPT を実施する。



実施主体	実施目的
舶用機器ベンダ	複数の開発機器がネットワーク化されたオンボードサブシステムに存在する脆弱性を明らかにする。
造船事業者	納入機器でネットワーク化されたオンボードシステムあるいはそのサブシステムが、実際に起こりうるサイバー攻撃に対しどの程度の耐性を有するのか技術的に検証する。
船社	運用されているオンボードシステムあるいはそのサブシステム、陸上施設のシステムと連携している場合は必要に応じて陸上施設も含めて、実際に起こりうるサイバー攻撃に対し現時点でどの程度の耐性を有するのか技術的に検証する。サイバー攻撃を検知した際の乗員や陸上施設における各担当者があらかじめ定められた動作を実行できるか、動作設計は適切であるかどうかについても検証する。

図 2.1.2　ペネトレーションテストの実施主体と実施タイミング

新造時の開発工程において舶用機器ベンダや造船事業者によって実施される従来の機器・システムテストは，被験機器・システムが設計通りに実装されており，期待される機能が正しく動作することを確認する目的で実施される。このため，テスト主体は被験機器・システムの開発に携わる要員となる。一方，新造時に実施する PT/TLPT は，被験システムの開発者･開発組織が設計段階において想定し得ない仕様上のサイバーセキュリティリスクを明らかにすることを目的に実施される。このため，テスト主体は被験システムの開発に携わらない第三者で，実際に生起し得るサイバー攻撃を模擬する力量を有する要員によって行われる。前述した新造時における PT/TLPT は被験システムの稼働直前状態で実施するが，本段階においてテストによりなんらかのサイバーセキュリティリスクが識別され，機器やシステムの仕様変更を余儀なくされるような事態が出来した場合，開発工程の大幅な手戻りとそれに伴う開発原価の超過，製品納期の延期といった事態が出来する。開発工程のどの段階において PT/TLPT を実施するかは被験組織の事情に沿って定めるところではあるが，被験システムの開発スケジュールと要工数については，PT/TLPT 実施による事業リスクを含めて計画する必要がある。

オンボードシステムやそれに接続する陸上設備内のシステムは，運用開始後にソフトウェアの更新やシステム運用手順の変更，一部新機器の導入といった様々なイベントが発生し，その内部状態は常に変化する。また，サイバー攻撃のテクノロジーも日々進化していることに鑑みると，運用開始後についても定期的に TLPT を実施することで現段階におけるシステムとその運用，組織のセキュリティマネージメントの健全性を確認することが重要である。

2.2 ペネトレーションテストの実施体制と手順，レッドチームの動作

2.2.1 実施体制

PT/TLPT を実行するにあたり，その実施体制には以下 5 つの機能を含める必要がある。

表 2.2.1 ペネトレーションテストに必要な機能

機能	役割
プロジェクト統括	PT/TLPT プロジェクトのオーナー組織。プロジェクトの目的と成果の設定、そのためのプロジェクト計画やテスト計画の設計、プロジェクトのための環境整備、プロジェクトの実行管理、成果のとりまとめ等を主管する。
被験製品・システム主管組織	被験製品・システムの主管組織で、被験製品・システムの開発時における PT/TLPT プロジェクトにおいては当該被験対象の開発主管組織が、当該被験対象の運用時における PT/TLPT プロジェクトにおいては当該被験対象の運用・保守主管組織が該当する。
レッドチーム	事前に設計された攻撃シナリオにそって、被験製品・システムに対し疑似サイバー攻撃を行う。必要に応じて攻撃シナリオの設計に関する助言も行う。
ホワイトチーム	プロジェクト統括による PT/TLPT プロジェクトの実行管理を支援する。レッドチームとブルーチームの関与を調整する役割を担う。テスト計画の設計、テスト実行中に生起する諸問題の解決、プロジェクトメンバー間でやり取りする情報の交通整理、テスト品質のコントロール等を支援する。
ブルーチーム （被験運用主管組織）	被験製品・システムに対するサイバー攻撃を検知した際に、あらかじめ定められた手順に従ってインシデントレスポンスを実施する運用組織で、サイバー攻撃に備え恒常的に設置されている組織。被験製品・システムの運用組織やインシデントレスポンスの実務を担う CSIRT 組織、インシデントレスポンスにおいて求められる各種経営判断を行うマネージメント組織等が含まれる。本組織は TLPT 実施時にのみ登場する。

PT の目的から，レッドチームは被験システムの設計や実装に携わらない第三者が担うこととなるが，日進月歩の攻撃技術に追随し，想定し得る攻撃者の力量と同等の力量を有するテスト担当者を被験組織自身で育成･雇用することは大きな負担となるため，ペネトレーションテストプロバイダ（以下，PT プロバイダ）と呼ばれる事業者へレッドチーム業務を委託するなどにより，レッドチームを調達することになる。委託費用の多寡や PT プロバイダが提供する支援内容につ

いては，テストプロジェクトの事情に応じて個別に折衝される事柄であるが，テスト品質を確保するうえで，なによりも PT プロバイダが提供するレッドチーム要員の専門的力量が求められる。レッドチーム要員の力量を示す指標としていくつかの第三者認定資格が存在するものの，これらの保有は必ずしも要員の技術力を保証しない。一般的に委託元であるテストユーザが，委託先の提供するレッドチーム要員の力量を見極めることは困難であるが，その力量を測る目安として以下を例示する。

- 世界的に著名なハッキングコンテストにおける優勝あるいは上位入賞といった事績の有無
- セキュリティ関連事業者，業界における評判
- 国防や大規模金融機関等，セキュリティのハイエンドユーザに対する案件実績の有無

ホワイトチームが役割を全うするためには，被験システムの仕様と運用，被験システム上で実行される業務とそれらに支障が生じた際の事業への影響，レッドチームが用いるテクノロジー，被験組織によるセキュリティマネージメントといった事柄に関して一定程度理解する必要がある。テストユーザが自組織内でそのような属性を有する要員を確保できない場合は，セキュリティベンダ等の第三者から調達することが選択肢となる。リスク分析や脆弱性診断といったサービスを提供しているセキュリティベンダであれば，テストユーザによるホワイトチーム運営を支援することが可能である。

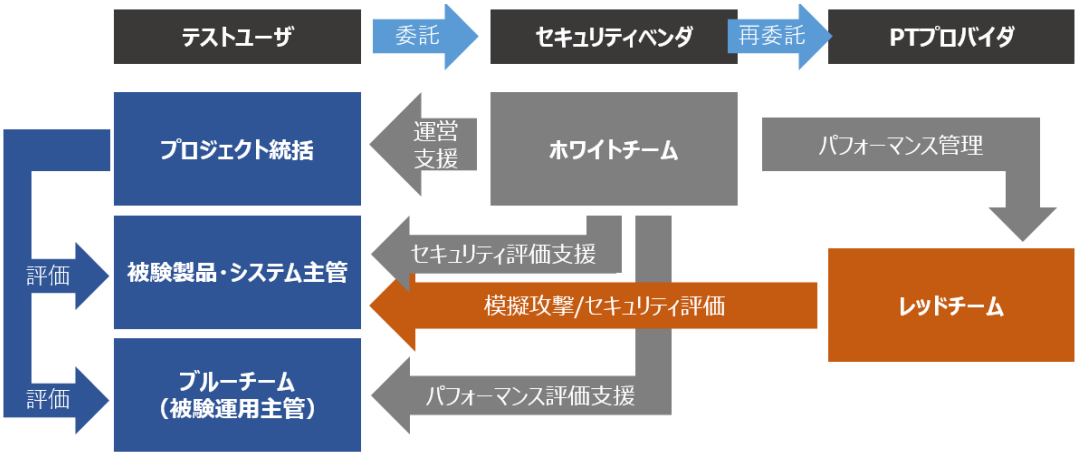


図 2.2.1　ペネトレーションテスト実施体制例

2.2.2 実施手順

PT/TLPT の実施工程は計画・準備，シナリオ構築，テスト実行，評価・改善計画策定の 4 工程に大別される。より詳細な手順や実施上の留意点については，公益財団法人金融情報システムセンターが 2019 年 9 月に発行した「金融機関等における TLPT 実施にあたっての手引書【PDF 版】」[1]に記載されている。当該手引書はテストユーザとして大規模金融機関を想定して記述されているが，他業種のテストユーザが PT/TLPT の手順を把握するうえでも参考となる内容となっている。

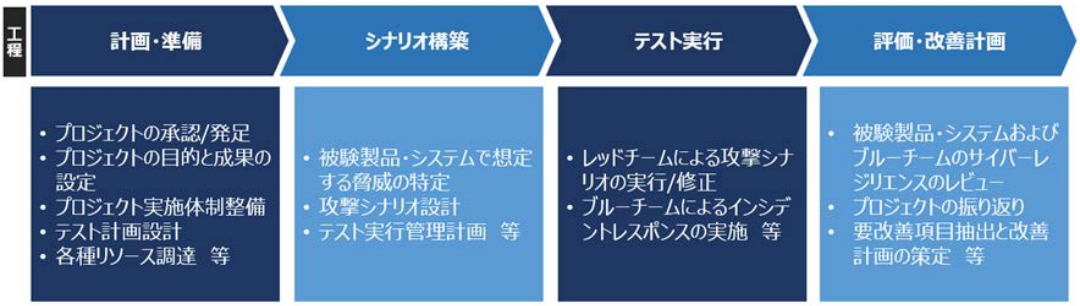


図 2.2.2 ペネトレーションテストの実施手順

2.2.3 レッドチームの動作

図 2.2.2 におけるテスト実行工程において，レッドチームは被験システムへの疑似攻撃に着手する。レッドチームによる疑似攻撃はサイバーキルチェーンと呼ばれる攻撃手順に従って実行されるが，レッドチームの動作は図 2.2.2 における計画・準備工程やシナリオ構築工程において設計されたテスト要件や制約事項，攻撃シナリオに合致していることが必要であり，これらはレッドチームに対して初期入力として与えられる。疑似攻撃の実行段階においてレッドチームは事前に定められたリソースにアクセスすることができる。このリソースには被験システムが具備する各種インターフェース，被験システムの仕様に関して一般に公開されている情報（カタログ情報やユーザマニュアルなど），被験システムの仕様に関する非公開情報（各種機器の設定値，ソフトウェア構成図など）等が含まれるが，どのタイミングでどのレベルでどのリソースにアクセスできるかといった制約については初期入力としてレッドチームに与えられる。レッドチームは疑似攻撃の最終段階が終了すると，実行結果とそれを示すエビデンスを出力することで疑似攻撃動作を終了する。

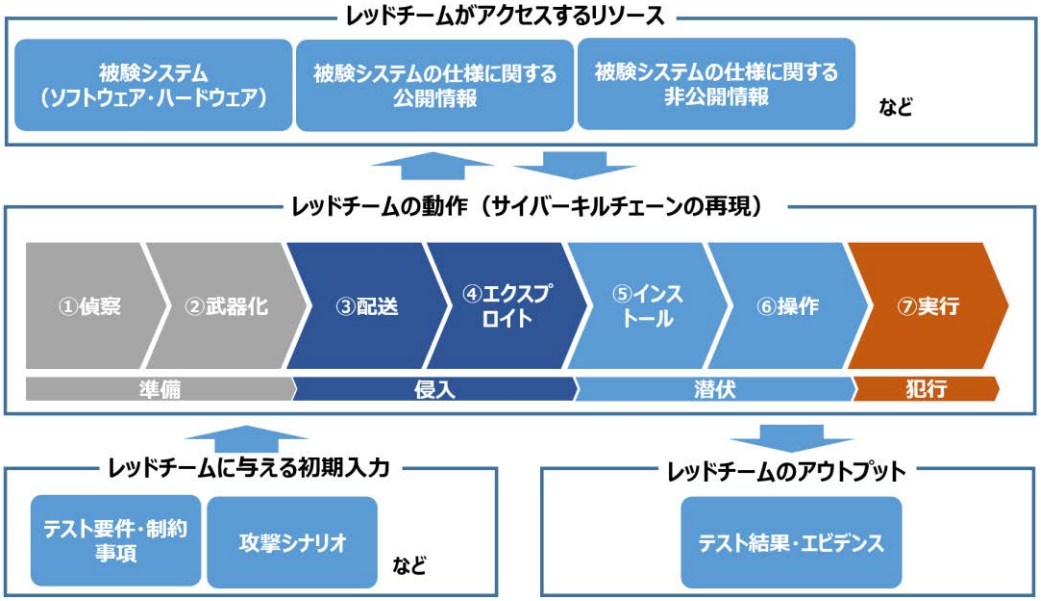


図 2.2.3 レッドチームの動作

[1] https://www.fisc.or.jp/publication/book/004197.php

表 2.2.2　サイバーキルチェーンの再現

プロセス	実行内容
①偵察	ソーシャルエンジニアリングや Web 調査による攻撃対象システムの周辺情報収集，攻撃対象システムが外部へ提供しているサービスを使った脆弱性スキャンなどを実施し，攻撃方法・手順設計のインプットとする。
②武器化	攻撃方法に適したツール（マルウェアなど）を準備する。
③配送	攻撃対象システム，あるいはそれに接続するノードに②で準備した攻撃用ツールを仕込む。例として標的型メール攻撃であれば，メールにマルウェアを添付して，メールの受領者に添付されたマルウェアファイルを実行させるなどの手段を用いる。
④エクスプロイト	攻撃対象システムに潜在する脆弱性や仕様の不備を利用するなどにより，より広く深く侵入を試みる。
⑤インストール	侵入した環境で，ツール（マルウェア）を継続的に実行するためのインストールや設定変更を行う。
⑥操作	ツールにより継続的に不正操作を可能とする状況を作り出す。
⑦実行	前工程を完了したのち，機密情報の窃取，システム可用性の毀損，ソフトウェア・ファイル完全性の毀損（改竄）といった攻撃目的を達成するための行動を実行する。

3 オンボードシステムへのペネトレーションテストの実施

3.1 実施概要

3.1.1 実施体制

本テストでは造船事業者による TLPT[2]を想定しているため，JMU および MTI をプロジェクト統括とし，ホワイトチームを NTT データ，レッドチームをイエラエセキュリティがそれぞれ担当している。テスト仕様やテストシナリオを決めるにあたっては船社である日本郵船の助言を受けた。また，試験結果の評価はプロジェクト統括と船級である ClassNK が共同で行った。

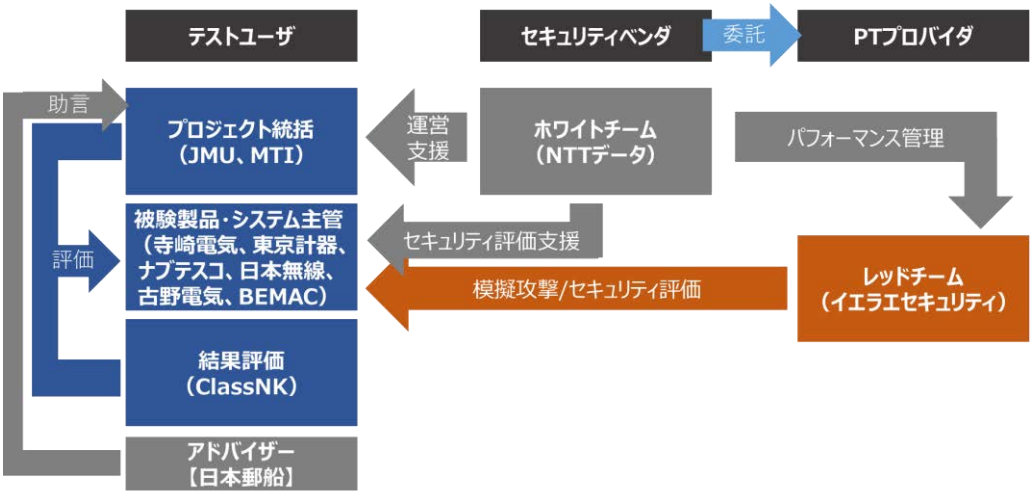


図 3.1.1 TLPT の実施体制

3.1.2 被験システムの選定

PT/TLPT は個々の機器がネットワーク化され，ある役割を担うシステムとして統合された段階で当該システムを対象に実施するものであり，船舶新造時には海事産業におけるシステムインテグレータ（造船事業者）が当該テストのメインユーザとなり，船舶の運航開始後は船社がメインユーザとなる。本プロジェクトでは船舶新造時に造船事業者が実施する TLPT を想定し，被験システムの選定と体制組みを行っている。被験システムの選定は以下の要件に従って実施している。

- 特定の船舶，船種に依存しない汎用的なシステム構成を有すること。
- 造船事業者側で構築する航海機器系システムおよび機関系システムを対象とし，船社個別に構築される情報系システムは対象外とすること。
- OT 機器 が接続されるネットワーク（以下，OT LAN）や船内 LAN によって各ノードがネットワーク化されているモダンなシステムであること。
- 本プロジェクトに参加する舶用機器ベンダの製品群で構成できるシステムであること。

上記要件により，被験対象とするシステムの構成を航海機器系システム(図 3.1.2)の 2 バリエーション及び機関系システム(図3.1.2)の 2 バリエーション，合計 4 バリエーションとしている。なお，テスト機材の調達や実験環境の都合により，各バリエーションについて個別にテストを行うこととしている。

[2] 2.1 節において TLPT では「規則・手順」や「人的対応」もテスト対象となる場合があると述べたが，それらは評価対象から除外し，「ソフトウェア/ハードウェア機能」のみを今回は評価対象とした。

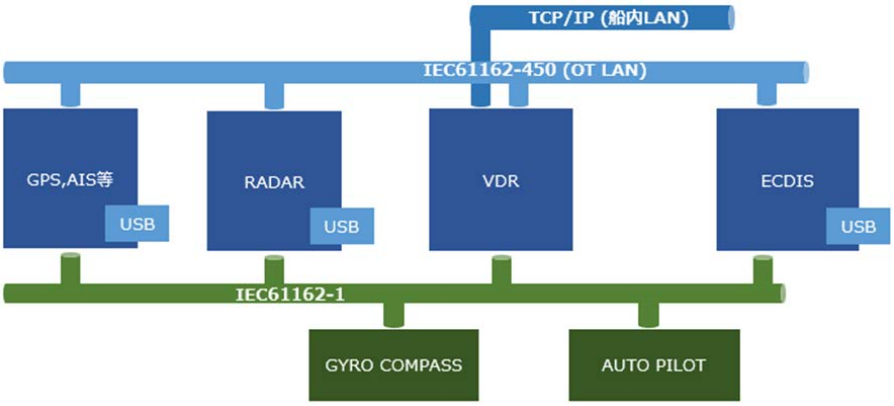


図 3.1.2　航海機器系被験システム構成図

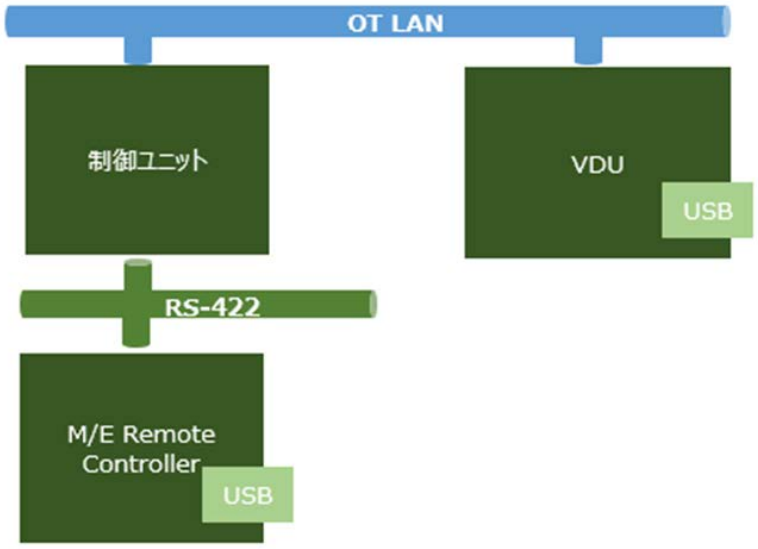


図 3.1.3　機関系被験システム構成図

3.1.3 レッドチームの攻撃手法と勝利の定義

本 TLPT におけるレッドチームの攻撃（または，「ゲーム」とも言う）を図 3.1.4 および表 3.1.1に示す。

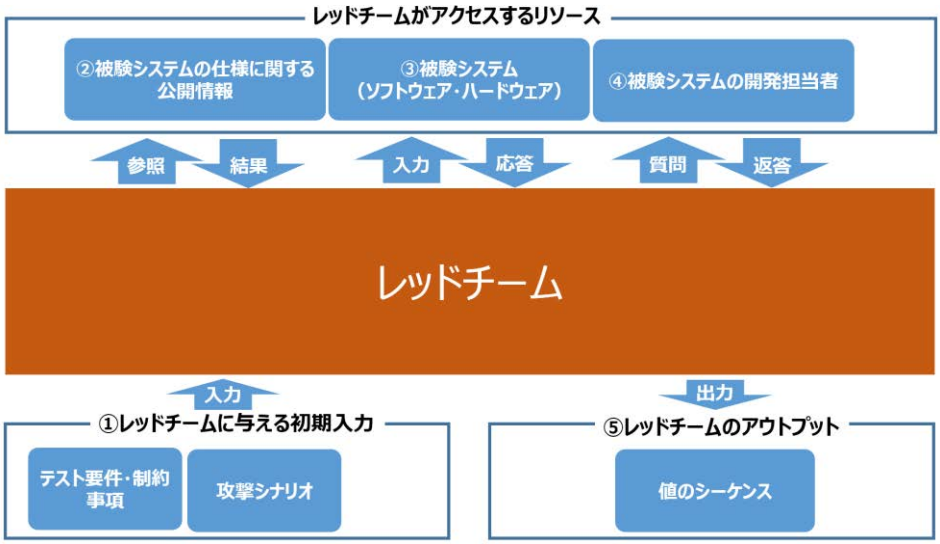


図 3.1.4 本 TLPT におけるレッドチームの攻撃

表 3.1.1 攻撃におけるレッドチームのアクション

アクション	概要
①初期入力の受領	本テストの要件，勝利条件と攻撃ルート・方法に関する制約（攻撃シナリオ），最終的な出力を得るまでに許容される上限時間を与える。本テストの共通要件として，レッドチームは被験システムが具備するインターフェースに対する論理的なアクセスのみが許容され，機器の物理的な分解・損壊を伴う解析は許容されないものとし，出力までの上限時間を 3 日間（計 24 時間）とする。被験システム下位構成毎の攻撃シナリオ，攻撃ルート，勝利条件については 3.2 章以降に記載する。
②公開情報へのアクセス	予め許容された時間内において，レッドチームは被験システム下位構成に関する公開情報（開示範囲が限定されていない情報）にアクセスすることができる。
③被験システムへのアクセス	予め許容された時間内において，レッドチームは被験システムにアクセスし，機器からの応答を得ることができる。アクセスする回数に制限はないが，初期入力で与えられたテスト要件や攻撃シナリオを逸脱する入力に対する応答は得られないものとする。
④被験システム開発担当者へのアクセス	予め許容された時間内において，レッドチームは必要に応じて被験システムを構成する各機器の仕様や設定について被験機器開発者へ質問し返答を得ることができる。このとき被験機器開発者は虚偽の返答（第三者の検証により

アクション	概要
	虚偽と判定される返答）は行わないものとする。開発担当者への質問回数に制限はないが，初期入力で与えられたテスト要件や攻撃シナリオを逸脱する質問に対する応答は得られないものとする。
⑤出力	予め許容された時間内において，レッドチームは任意の値のシーケンスを出力する。

表 3.1.1 に記載した動作を実行するレッドチームが以下に列記する要件 a および要件 b をすべて満たす場合，レッドチームは所与の攻撃シナリオにおいてブラックボックスゲームに勝利したと定義し，要件 a のみを満たす場合をグレーボックスゲームに勝利したと定義する。

a. 所与の上限時間内に所与の攻撃シナリオで規定される勝利条件を満たす出力を得る。
b. 攻撃において，被験機器開発担当者から得た情報は皆無である。

グレーボックスゲームは，実際の攻撃者がなんらかの手段をもって被験システムに関わる非公開情報へアクセスできる状況を想定するものである。たとえば，攻撃対象であるシステムの開発ベンダの従業員に標的型攻撃メールを仕掛け，アカウントハッキングなどにより組織内のファイルサーバーにアクセスし，攻撃対象システムの仕様に関する機密情報を窃取するなどの準備行動を攻撃者が行うことは十分に想定されることである。また，中古・転売マーケットを通じて攻撃対象システムを構成する機器を購入し，リバースエンジニアリングを行うことでより多くの攻撃に有用な情報を引き出すといったことも想定される。組織による機密情報の管理やサプライチェーンの管理には限界があり，多くのサイバー攻撃が管理上の不備・限界を利用して行われている実態がある。本テストにおいて，レッドチームに被験システム開発担当者へのアクセスを与えるのはこのような状況を想定するためである。

3.1.4 本テストにおけるレッドチームのアクションに関する前提と制約

サイバー攻撃を企図する第三者は，Web 等で広く公開されている情報をインターネット経由で入手する，ソーシャルハッキングと呼ばれる手法等を用いて特定人物の認証情報を取得し，対象攻撃システムの仕様を管理している組織の IT リソースへ不正にアクセスすることで非公開情報を入手する，標的型メール攻撃等を用いて攻撃対象システムの仕様を管理している組織の OA 環境へ不正にアクセスし非公開情報を入手するなどといった手口を用いて攻撃に利する情報を収集するが，本テストにおいてレッドチームによる非公開情報へのアクセスは被験システム開発担当者経由のみと制限する。また，今回は 3 日間という攻撃時間を考慮し，被験システムに関する公開情報についてはゲーム開始前にレッドチームに与えるものとしている。

3.1.5 攻撃シナリオの設計要件

本テストは脅威ベースのペネトレーションテストであるため，攻撃シナリオ設計するにあたってまず始めに，誰にとって，どのようなタイミングで発生する，どのような脅威を想定するのか明らかにする必要がある。本テストでは船舶が外洋航行中に第三者からサイバー攻撃を受けるというユースケースを想定し，攻撃シナリオの設計要件として以下を設定している。

- 攻撃を行う第三者はなんらかの手段をもって被験システムのインターフェースにアクセスできる状態にある。衛星回線を経由した遠隔でのアクセスは，通常船社個別に構築されている情報系ネットワークに設置されている各種セキュリティ機能を突破する必要があるが，本テストではそれを考慮しない。
- 脅威の特定に際しては，船舶の安全運航を大きく毀損する直接的，間接的インシデントを想定する。
- 船舶の出航前（あるいは出荷前）状態において，オンボードシステムの状態は健全であるとし，新造時のサプライチェーンを狙った攻撃，開発者や保守者を狙った攻撃などを通じた第三者による不正アクセスは一切行われていないものとする。

- 船舶の乗員や陸上設備の要員など，オンボードシステムへのアクセスが認められている人員，船舶の運航に携わる人員が，オンボードシステムに対して意図的にサイバー攻撃を行うことはないものとする。
- 攻撃者は攻撃対象となるオンボードシステムへ物理的にアクセスすることはできないものとする。

本テストでは上記の設計要件を踏まえ，JMU および MTI が主体となり，NTT データやイエラエセキュリティの支援を受けつつ，被験システム下位構成毎に攻撃シナリオを設計している。

3.1.6 被験システム主管の負担

本プロジェクトでは 4 バリエーションの被験システム下位構成ごとにテストを実施することとしているため，古野電気，日本無線，寺崎電気，BEMAC の各社がそれぞれ被験システム主管となっている。通常，被験システム主管には以下のタスクが発生する。

- テストを実施することに関する組織内の意思決定
- テスト実施に伴う各種支出の承認
- テスト実施に伴う情報，機材，要員，テスト環境の調達
- テスト実施体制の構築
- 提供機材，提供環境，提供情報に関する条件整理
- テスト環境における機材の設営と設定
- 機材の撤収とテスト環境のクローズ
- テスト結果の評価と経営層への報告
- 各種事務手続き，契約手続きの実施

被験システム主管がテストのオーナーシップを有する場合，要員の調達にはレッドチーム要員やホワイトチーム要員も含まれる。仮に舶用機器ベンダが自社製品の開発工程においてペネトレーションテストを実施する場合，上記に必要な労務費，物品費，間接費のほかにレッドチームなどの外注費が必要となってくる。

3.1.7 実施スケジュール

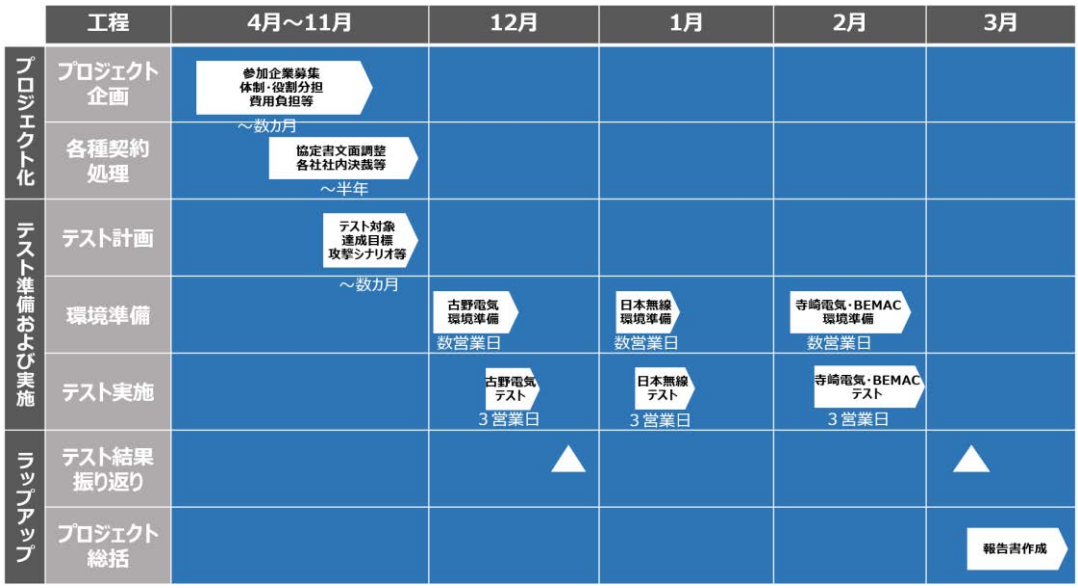


図 3.1.5 本 TLPT の実施スケジュール

3.2 航海機器系システム試験内容

3.2.1 実施期間および実施環境

航海機器系システム試験の実施期間及び実施環境を以下に示す。

表 3.2.1 航海機器系システム実施期間及び実施環境

被験システムベンダー	古野電気(株) 東京計器(株)	日本無線(株)
実施期間	2019 年 12 月 9 日，10 日，11 日	2020 年 1 月 8 日，9 日，10 日
被験システム設営場所	古野電気（株）東京支社 〒101-0024 東京都千代田区神田和泉町 2-6 今川ビル	日本無線(株) 辰巳事業所 〒135-0053 東京都江東区辰巳 1-7-32
被験システム開発主管組織	古野電気（株）舶用機器事業部 開発設計統括部開発部基盤技術開発課	日本無線(株) マリンシステム事業部 情報ビジネス技術部
被験システム構成機器	FMD-3200(ECDIS) VR-7000(VDR) GP-170(GPS) TG-8000(GYRO COMPASS)	JCY-1900 (VDR) JAN-9201 (ECDIS) JMR-9200 (RADAR) JLR-8600 (GPS) JHS-183 (AIS)

3.2.2 攻撃シナリオと攻撃の勝利条件

当該被験システム下位構成においては，表 3.2.1 に記載する 3 つの攻撃シナリオとレッドチームの勝利条件を設計している。各勝利条件は，外洋航行中の船舶の安全運航を毀損させる重大なインシデントの発生に該当している。

表 3.2.2 攻撃シナリオと勝利条件

シナリオ	攻撃	勝利条件
シナリオ 1	なんらかの手段をもって船内 LAN にアクセス可能な攻撃者が，船内 LAN に接続する VDR に LAN ポートから不正アクセスする。次に攻撃者は VDR を踏み台として ECDIS へ不正アクセスし，なんらかの手段をもって ECDIS に対し不正な制御信号を送信させる，もしくは ECDIS や VDR の内部状態を変更することにより，船舶の安全航行に重大な支障をきたす状況を招く。	攻撃開始から 3 営業日以内に以下のいずれかを満たす値のシーケンスを出力する。 ・ ECDIS から不正な制御信号を送信する。 ・ 船舶の安全航行に重大な支障をきたす状況を招く程度に ECDIS や VDR の内部状態を変更する。
シナリオ 2	攻撃者はなんらかの手段で乗員（ECDIS ユーザ）が業務で使用する USB メモリにマルウェアを仕込む。乗員が業務を実行するために当該 USB メモリを ECDIS に接続する。これにより攻撃者は ECDIS へ不正アクセスし，なんらかの手段をもって ECDIS に対し不正な制御信号を送信させる，もしくは ECDIS の内部状態を変更することにより，船舶の安全航行に重大な支障をきたす状況を招く。	攻撃開始から 3 営業日以内に以下のいずれかを満たす値のシーケンスを出力する。 ・ ECDIS から不正な制御信号を送信する。 ・ 船舶の安全航行に重大な支障をきたす状況を招く程度に ECDIS の内部状態を変更する。

シナリオ	攻撃	勝利条件
シナリオ 3	なんらかの手段をもって OT LAN にアクセス可能な攻撃者が，OT LAN に接続する ECDIS に LAN ポートから不正アクセスし, なんらかの手段をもって ECDIS に対し不正な制御信号を送信させる，もしくは ECDIS の内部状態を変更することにより，船舶の安全航行に重大な支障をきたす状況を招く。	攻撃開始から 3 営業日以内に以下のいずれかを満たす値のシーケンスを出力する。 ・ ECDIS から不正な制御信号を送信する。 ・ 船舶の安全航行に重大な支障をきたす状況を招く程度に ECDIS の内部状態を変更する。

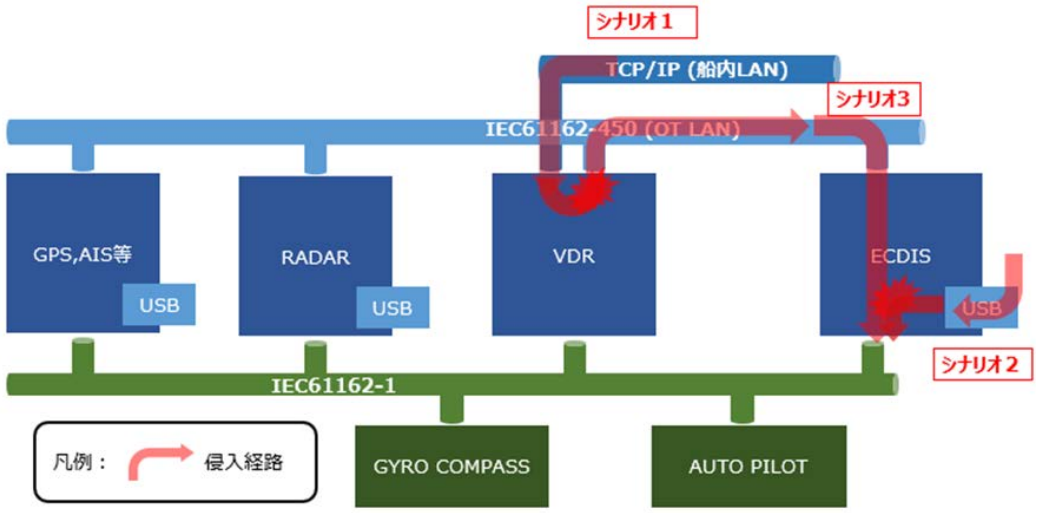


図 3.2.1 被験システムの構成とサイバー攻撃によるシナリオ別侵入経路

オンボードシステムへの侵入を試みる第三者による攻撃シナリオは，生起する蓋然性の高さで降順にシナリオ 2，シナリオ 1，シナリオ 3 になるものと想定される。

外洋航海中の船舶において，乗員が ECDIS に USB メモリでアクセスするという業務が存在する。過去陸上設備では，厳格に管理されていない USB メモリによるマルウェア感染という事態が頻繁に出来しており，ECDIS の USB ポートが攻撃者のエントリポイントとなる蓋然性は他のシナリオにおけるそれと比較して十分に高い。

衛星通信等を介して船内設備へ侵入を試みる場合，OT LAN は船内 LAN の先に存在する LAN であり，OT LAN へアクセスするためには先行して船内 LAN へアクセスし，OT LAN と船内 LAN の境界ノードである VDR のセキュリティ機能を突破する必要がある。シナリオ 3 はこのプロセスに攻撃者が成功したという前提にもとづいたシナリオであり，シナリオ 1 と比して強い仮説に基づくシナリオとなっている。

3.3 機関系システム試験内容

3.3.1 実施期間及び実施環境

機関系システム試験の実施期間及び実施環境を以下に示す。

表 3.3.1 機関系システム試験の実施期間及び実施環境

被験システムベンダ	寺崎電気産業(株) ナブテスコ(株)	BEMAC(株)
実施期間	2020 年 2 月 4 日，5 日	2020 年 2 月 18 日，19 日
被験システム設営場所	寺崎電気産業(株)　東京営業所 〒103-0025 東京都中央区日本橋茅場町 1-6-10 日幸茅場町ビル	(一財)日本海事協会　管理センター別館 〒102-0094 東京都千代田区紀尾井町 3-3
被験システム開発主管組織	寺崎電気産業(株)　海洋技術部　海洋設計 2 課 ナブテスコ(株)　舶用カンパニー 技術部 技術戦略推進グループ	BEMAC(株)　イノベーション本部　IT イノベグループ
被験システム構成機器	TERANET 50X PCU(制御ユニット) Marine Computer II(VDU) M-800-V (M/E Remote Controller)	BE-D11 BD-ETH02/BD-MMC02/BD-MPS02(制御ユニット) VDU Security Device

3.3.2 攻撃シナリオと攻撃の勝利条件

当該被験システム下位構成においては，表 3.3.2 に記載する 3 つの攻撃シナリオとレッドチームの勝利条件を設計している。各勝利条件は，外洋航行中の船舶の安全運航を毀損させる重大なインシデントの発生に該当している。

表 3.3.2 攻撃シナリオと勝利条件

シナリオ	攻撃	勝利条件
シナリオ 1	なんらかの手段をもって OT LAN にアクセス可能な攻撃者が，OT LAN に接続する VDU または制御ユニットの LAN ポートより不正アクセスし，なんらかの手段をもって制御ユニットに不正な制御信号を送信させる。	攻撃開始から 3 営業日以内に以下を満たす値のシーケンスを出力する。 ・ 制御ユニットに不正な制御信号を送信させる。
シナリオ 2	攻撃者はなんらかの手段をもって乗員（VDU ユーザ）が業務で使用する USB メモリにマルウェアを仕込む。乗員は業務を実行するために当該 USB メモリを VDU に接続する。これにより攻撃者は VDU を踏み台として制御ユニットへ不正アクセスし，なんらかの手段をもって制御ユニットに不正な制御信号を送信させる。	攻撃開始から 3 営業日以内に以下を満たす値のシーケンスを出力する。 ・ 制御ユニットに不正な制御信号を送信させる。
シナリオ 3	攻撃者はなんらかの手段をもって乗員（M/E Remote Controller ユーザ）が業務で使用する USB メモリにマルウェアを仕込む。乗員が業務を実行するために当該 USB メモリを	攻撃開始から 3 営業日以内に以下のいずれかを満たす値のシーケンスを出力する。 ・ M/E Remote Controller に不

シナリオ	攻撃	勝利条件
	M/E Remote Controller に接続する。これにより攻撃者は CDP へ不正アクセスし，なんらかの手段をもって M/E Remote Controller に不正な制御信号を送信する，もしくは M/E Remote Controller の内部状態を変更することにより，船舶の安全航行に重大な支障をきたす状況を招く。	正な制御信号を送信する ・ 船舶の安全航行に重大な支障をきたす状況を招く程度に M/E Remote Controller の内部状態を変更する

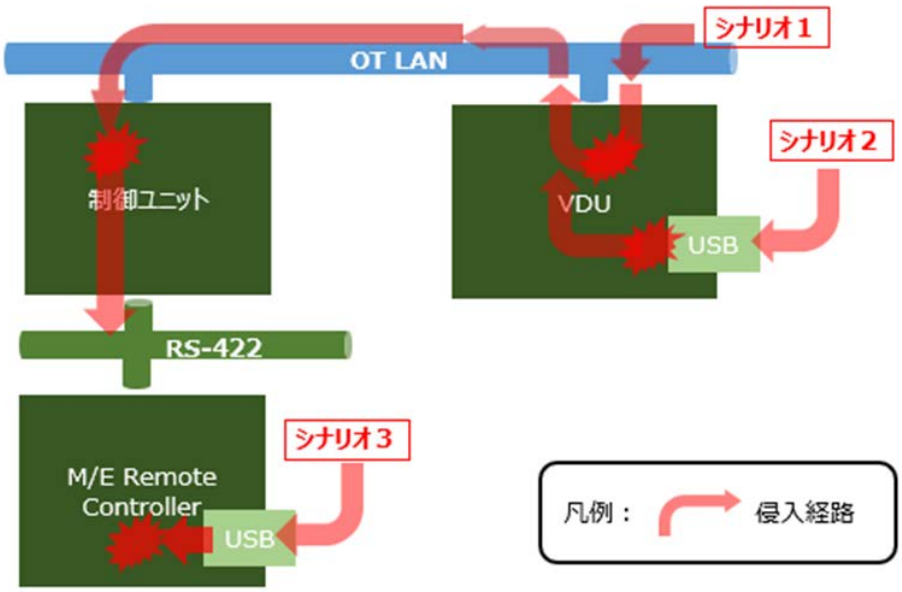


図 3.3.1 被験システムの構成とサイバー攻撃によるシナリオ別侵入経路

4 まとめと考察

本プロジェクトでは，船舶サイバーセキュリティ対策において，Security by Design の観点で，今後要求されるであろう機能要件が正しく実装されているかを「検証」する手段について，船社，船級，造船事業者，舶用機器ベンダが連携し，さらにサイバーセキュリティの専門家の協力を得ながら検討を行った。

具体的には，新造船建造時に，船社，船級，造船事業者や舶用機器ベンダが今後どのように「検証」をしていくべきかを，既存の船上機器・システムに対して PT を実施する形でおこなった。

特に，本プロジェクトでは，就航後の船舶運航におけるサイバーリスクの低減を念頭において，何が船舶安全運航上クリティカルなインシデントであるかを考慮したうえで，事前準備を関係者間で十分に議論し実施することにより，4.1 節に示すように，「検証」おける PT 実施の有効性が十分にあることを確認した。また，オンボードシステムへの PT で特に準備が必要な事項について，4.2 節に示す知見を得た。

さらに，今後，海事業界として引き続き検討すべき項目とアクションについて，4.3 節にまとめた。

4.1 PT の効果

今回の PT の結果，多くのケースでは今回の指定期間内の攻撃は成功しなかったものの，下記を達成するケースも少数例ながら存在した。

- 当該機器上のソフトウェアの動作を停止させる
- 当該機器上の情報やデータを閲覧・改ざんする
- 当該機器から接続される LAN 内へ不正な制御通信を送信可能な状態とする

本節では，PT の「検証」における効果として，攻撃の結果明らかになったレッドチームの攻撃行動への対策の一例を 4.1.2 項で，今後の検討が必要な事項とその対応例を 4.1.3 項で説明する。それらの前提として，今回の PT においてレッドチームが被験製品に対してどのような攻撃を行ったのかを 4.1.1 項で説明する。

4.1.1 オンボードシステムに対するレッドチームの攻撃行動

3.1.3 項にてレッドチームの攻撃手法とアクションについて説明した。ここでは，実際の攻撃においてレッドチームがオンボードシステムに対して，具体的にどのような攻撃行動を行ったのかを攻撃経路別に説明する。

なお，以降の記載は海事業界内で汎用的に役立つ情報となるよう，固有の機器名称や型番は伏せた上で，可能な範囲で一般化していることに留意いただきたい。また，実際の攻撃においては機器・システム別に異なる攻撃行動についても，一部一般化し記載している。

【USB 経由の攻撃】

① 機器 USB ポートにキーボードを接続し，特殊キー/ショートカットキーの入力を受け付けているかどうかを把握する。
② 入力を受け付けている場合，キーボード操作を模擬できる BadUSB[3]を用いて当該機器に対して侵入を試みる。
③ 機器への侵入が成功した場合，当該機器の内部状態を変更する。または不正な制御通信を送信する。このとき，製品が汎用的な OS・ミドルウェアを利用している場合，それらの既知の脆弱性を利用する。

【船内 LAN（IT/OT）経由の攻撃】

① 機器の公開ポート/サービスを調査する。
② 公開されているポート/サービスを発見した場合，それらに対して接続を試みる。
（ア）接続に際して認証情報が必要な場合，製品の設定ファイルやマニュアル等の公開情報から認証情報を探索する。
（イ）汎用的な接続インターフェースの場合，既知の脆弱性を利用して接続を試みる。
③ 機器に接続できた場合，当該機器の内部状態を変更する。または不正な制御通信を送信する。このとき，製品が汎用的な OS・ミドルウェアを利用している場合，それらの既知の脆弱性を利用する。

[3] BadUSB とは, USB 接続で利用するデバイス(usb メモリなど)にあらかじめ悪意のあるコードを書き込み USB 接続時にコードを走らせ何らかの悪質な動作をさせる攻撃手法。ここでは，当該の攻撃手法で用いられる USB メモリのことを意味する。

4.1.2 レッドチームの攻撃行動への対策例

今回のテストにおいて，4.1.1 節で説明したレッドチームの攻撃行動からゴール達成を防ぐことに貢献した対策の一例は表 4.1.1の通りである。

表 4.1.1 今回の PT におけるレッドチームの攻撃行動への対策例

大分類	小分類	レッドチームへの攻撃行動への対策例
REDS セキュリティ		キーボード操作を模擬できる BadUSB を用いて侵入を試みたが，BadUSB からの文字列入力はアプリケーションに入力されたため，任意コマンドの実行には失敗した。
ソフトウェアメンテナンス		OS/インターフェースに既知の脆弱性が存在しなかった。
ユーザ認証/認可	認証実施	ある航海機器が提供するサービスにはすべて認証が求められており，認証情報についても容易に入手できないよう設定・管理されていた。
	権限設定	提供するサービスへアクセスするアカウントに与えられる権限を限ることで，当該アカウントで実施できる操作を限定している。
公開設定	適切なポート/サービス公開	必要最低限のサービスのみを提供しており，不要なサービスは提供していない。このことにより，レッドチームのエントリポイントが限定された。
	適切なファイル公開	レッドチームは，当該機器から電文を発出する操作を実現するための情報収集を当該機器内のファイルを閲覧することによって行うが，公開サービスのアカウントで閲覧できるファイルは限定されている。

次項では，攻撃成功につながってしまった今後の検討が必要な事項について説明する。

4.1.3 今後の検討が必要な事項とその対応例

今後の検討が必要な事項と，その事項が生じている背景は表 4.1.2 の通りである。なお，いずれの事項も現時点では，規格や船級規則等の仕様では要求されていない点に留意が必要である。

表 4.1.2 今回の PT で明らかになった検討事項とその背景

大分類	小分類	明らかになった検討事項	背景
REDS セキュリティ		USB ポートから特殊キー操作が有効	メンテナンス用途で，USB キーボード，マウスでの操作が必要
ソフトウェアメンテナンス		Windows ベースの機器に，既知の Windows の脆弱性が存在	OS をアップデートした際の動作確認等が煩雑
ユーザ認証/認可	認証の不備	● 同一 LAN 内であれば重要なデータが存在する領域に匿名アクセスが可能 ● 認証なしで重要な機能へアクセス可能 ● Windows の管理者アカウントにパスワードが設定されておらず，ネットワーク経由でファイル読み書き可能	● 船内へアクセス可能な人物は限られており，認証の必要性が感じられない ● 認証を必要とした場合，個船毎のアカウント情報管理が煩雑になり，メンテナンス上困難
	権限設定の不備	機器管理画面において，Guest アカウントで Administrator アカウント権限と同様の操作が可能	厳密に権限を管理する場合，個船毎のアカウント情報管理が煩雑になり，メンテナンス上困難
	貧弱な ID/パスワード	デフォルトのパスワード，もしくは容易に推測可能なパスワードを設定	厳密にパスワードを管理する場合，個船毎のアカウント情報管理が煩雑になり，メンテナンス上困難
公開設定	不要なポート/サービス公開	公開不要なポート/サービスを公開	● システム構築/設定時の考慮漏れ ● 設定変更作業時の戻し忘れ
	不要なファイル公開	● 公開不要な機器上のファイルが外部から閲覧可能 ● ディレクトリリスティング機能が有効になっておりファイル一覧情報を取得可能 ● 企業のウェブサイト上に，公開を想定していない機器関連情報のファイルを公開	機器の設置・メンテナンスのための情報を迅速に得られるようにするため

今後は，上記事項への対応及びその対応が適切であるかどうかを検証する方法が求められる。具体的には，以下 3 つの観点から検討していくことが望ましい。

- 脆弱性の存在を前提としつつ，インシデントにつながらないように人的な対策を行う「運用の観点」。
- 機器の機能面から対応を進めていく「機能実装の観点」。
- 「機能実装の観点」「運用の観点」両方の観点からの対応が十分に行われていることを確認する「検証の観点」。

表 4.1.3 では，「運用の観点」および「機能実装の観点」からの対応例を整理した結果を示す。なお下表の BIMCO ガイドラインとは，BIMCO 等によりに出版された”THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS ver3”を意味する。

表 4.1.3 今回の PT で明らかになった検討事項と想定される対応例

大分類	小分類	明らかになった検討事項	「運用の観点」の対応例	「機能実装の観点」の対応例	BIMCO ガイドライン参考箇所
REDS セキュリティ		USB ポートから特殊キー操作が有効	USB ポートブロック 業務用 USB メモリの管理徹底	特殊キー入力を受け付けない/特定の入力のみ受け付ける機能の実装	5.2 Technical protection measures Physical security 5.3 Procedural protection measures Training and awareness Physical and removable media controls
ソフトウェアメンテナンス		Windows ベースの機器に，既知の Windows の脆弱性が存在	OS，ミドルウェアの定期的なアップデートの実施	出荷前の OS, ミドルウェアのアップデート 独自 OS, ミドルウェアの利用	5.2 Technical protection measures Application software security (patch management) 5.3 Procedural protection measures Upgrades and software maintenance
ユーザ認証/認可	認証の不備	● 同一 LAN 内であれば重要なデータが存在する領域に匿名アクセスが可能 ● 認証なしで重要な機能へアクセス可能 ● Windows の管理者アカウントにパスワードが設定されておらず，ネットワーク経由でファイル読み書き可能	ユーザ認証ポリシーの策定とポリシーに基づく認証設定	ユーザ認証ポリシーに基づき設定が可能な認証設定機能の実装	5.3 Procedural protection measures Training and awareness Use of administrator privileges
	権限設定の不備	機器管理画面において，Guest アカウントで Administrator アカウント権限と同様の操作が可能	権限設定ポリシーの整備とポリシーに基づく権限設定の実施	権限設定ポリシーに基づき権限が設定可能な機能の実装 権限の設定状況を確認する機能の実装	5.2 Technical protection measures Secure configuration for hardware and software 5.3 Procedural protection measures Training and awareness Use of administrator privileges
	貧弱な ID/パスワード	デフォルトのパスワード，もしくは容易に推測可能なパスワードを設定	パスワードポリシーの整備とポリシーに基づくパスワード設定の実施	パスワードポリシーに基づきパスワードが設定可能な機能の実装	5.3 Procedural protection measures Training and awareness Use of administrator privileges
公開設定	不要なポ	公開不要なポート/サービスを公開	ポート/サービスの公開状況の把	公開不要なポート/サービス	5.2 Technical protection measures

大分類	小分類	明らかになった検討事項	「運用の観点」の対応例	「機能実装の観点」の対応例	BIMCO ガイドライン参考箇所
	ート/サービス公開		握と公開不要なポート閉鎖/サービス停止	が公開されていることを検知する機能の実装	Limitation to and control of network ports, protocols and services
	不要なファイル公開	● 公開不要な機器上のファイルが外部から閲覧可能 ● ディレクトリリスティング機能が有効になっておりファイル一覧情報を取得可能 ● 企業のウェブサイト上に，公開を想定していない機器関連情報のファイルを公開	ファイルの公開状況の把握と公開不要なファイルの公開停止	公開不要なファイルが公開されていることを検知する機能の実装	—（該当箇所無し）

4.2 PT 実施体制・手順などの知見

テストの計画・準備・シナリオ構築工程においてテストユーザが考慮すべき事項と実行手順については，「金融機関等における TLPT 実施にあたっての手引書【PDF 版】」にその概要が記載されているが，特に本プロジェクトの実施を通じて明らかになった留意事項を，今後の知見として以下に記す。

- テストユーザがレッドチームやホワイトチームを第三者サービスによって調達する場合，レッドチームやホワイトチームが知り得た被験システムやユーザ業務に関する情報，レッドチームが有するテスト・攻撃ノウハウの開示粒度等，各種情報・ノウハウに関する取扱い，レッドチームが作成する中間成果物や最終成果物のコピーライトに関する取扱い等について事前に認識を合わせる必要がある。
- レッドチームの作業状況によっては，シナリオ変更に伴う被験システムの仕様や設定に関する追加的な情報提供の要望，機器に対する特定の攻撃（操作）の可否に関する判断の要望等が ad hoc に発生する。このため，被験システムの仕様に精通している技術者や，特にテスト対象が本番システムとなる場合においては操作の可否についてエキスパートの助言を受けながら事業継続性の観点から判断できる責任者などのテストユーザ側要員をテスト実施体制に含めるとともに，それらの要員が ad hoc に発生するレッドチームの要望を迅速に処理できるよう計らうことが重要である。
- レッドチーム，ホワイトチーム，テストユーザといった各担当者，チーム間でのコミュニケーション手段について事前に定め，その利用に伴う手続きについて整理しておく必要がある。テスト中はレッドチームによる作業の進行状況に合わせて，レッドチーム，ホワイトチーム，テストユーザ間で多くの即時的なコミュニケーションが発生する。このようなコミュニケーションにはメールや電話といったオールドメディアよりもクラウドサービス型ビジネスチャットツールが適しており，本プロジェクトにおいてもビジネスチャットツールを活用している。一方で，クラウドサービス型のコミュケーションツールの利用については，そのサービス仕様等がテストユーザにおける既存の情報セキュリティ規定に合致しない，あるいはビジネスチャットツールの利用を想定しておらずユーザの IT 環境や業務設計が対応していないといったことも起こり得る。
- レッドチームによる疑似攻撃によっては，被験システムの内部状態が変更（既存ファイルの書き換えや削除，攻撃用実行ファイルの配置，攻撃によるシステムやアプリケーションログへの影響など）される，システムが想定外の動作をする，場合によっては被験システムの一部が損壊するといった事態が出来し得る。これらの生じうる事象についてどのように対処するのか，被験システムの原状復帰を求めるのか，求めるのであればだれがどのような手順で実施するのか，当該事象についてテストユーザとレッドチームとの間の責任分界をどのように考えるかといった事柄について事前に認識を合わせる必要がある。
- 被験システムが本番運用されているシステムである場合や，大規模で物理的な制約が生じる場合など，被験システムの物理的な所在地が制約される場合は，レッドチームによる被験システムへのアクセス方法や手順を事前に設計しておく必要がある。たとえばオンサイトでテストを行う場合には特定区画への立ち入り許可，テスト中の安全管理方法といったことを，リモートアクセスによってテストを行う場合には，リモートアクセス用の環境設営やアクセス方法・管理方法の設計などが必要となる。
- 攻撃シナリオを設計するにあたり，まず定められるべきはテストユーザにとっての脅威とはなにかということであるが，テストユーザ毎に脅威は異なる。舶用機器ベンダ，造船事業者，船社にとって事業継続性を毀損させうる脅威は必ずしも同一ではない。舶用機器ベンダや造船事業者が脅威を定める場合，機器やシステムのユーザである船社のオペレーションを理解し，船社が想定する脅威を考慮に入れる必要がある。従って脅威を定める工程においては船社業務や船社が想定する脅威に精通した人材を作業体制に含めることに配慮する必要がある。

4.3 PT 実施要件として今後検討すべき事項

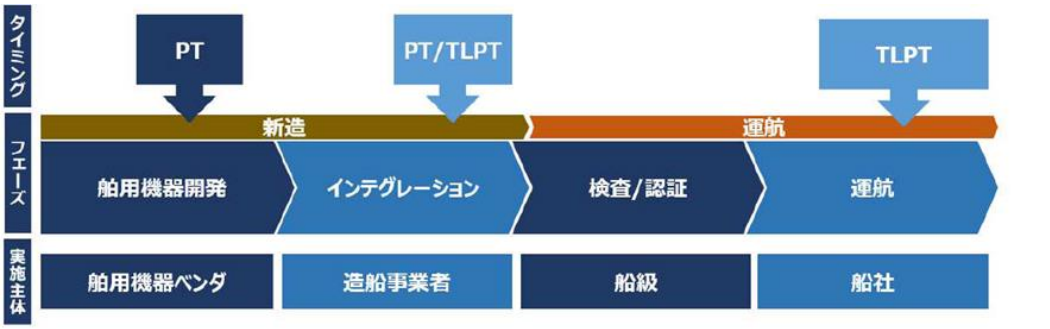
4.3.1 今後の検討が必要な項目の全体像

船舶サイバーセキュリティ対策での，Security by Design の観点における，機能要件や運用要件が適切に実装されているか検証する手段として PT の実施を企図する場合，実施計画において下記を明らかにする必要がある。

- When：PT の実施タイミング
- Where：PT の実施場所

- Who：PT の実施主体
- What：PT で検証する運用/機能の要件
- Why：PT の実施目的
- How：PT の実施方法

このうち，オンボードシステムへの PT の実施については，When（タイミング）と Who（実施主体）と Why（実施目的）は以下のような関係があり，いずれか 1 つが決まれば他の要素も自然と決定する。また，Where（実施場所）も実施タイミングに依存する。



実施主体	実施目的
舶用機器ベンダ	複数の開発機器がネットワーク化されたオンボードサブシステムに存在する脆弱性を明らかにする。
造船事業者	納入機器でネットワーク化されたオンボードシステムあるいはそのサブシステムが、実際に起こりうるサイバー攻撃に対しどの程度の耐性を有するのか技術的に検証する。
船社	運用されているオンボードシステムあるいはそのサブシステム、陸上施設のシステムと連携している場合は必要に応じて陸上施設も含めて、実際に起こりうるサイバー攻撃に対し現時点でどの程度の耐性を有するのか技術的に検証する。サイバー攻撃を検知した際の乗員や陸上施設における各担当者があらかじめ定められた動作を実行できるか、動作設計は適切であるかどうかについても検証する。

図 4.3.1　PT の実施主体と実施タイミング（再掲）

次に What（検証対象）については，現在 IACS や IMO において現在策定された/されつつある運用/機能要件が該当するため，本プロジェクトのスコープ外である。また，How については What をはじめとする他の 5W が確定したあとに議論することになる。

以上のことから，本プロジェクトの結果を踏まえた今後のアクションとしては，次項に示すように，PT 実施タイミングの決定に資するアクションを起こすことが重要である。

4.3.2　PT 実施タイミングの検討と今後のアクション

2.1 節で記載した通り，オンボードシステムのライフサイクルにおいて PT を実施するタイミングと実施主体については以下が想定される。

① 舶用機器群で構成されるシステムを造船事業者へ納入する前段階において，当該システムを開発した舶用機器ベンダによって PT を実施する。
② 各舶用機器ベンダより納入された機器群をインテグレートし，オンボードシステムを稼働直前状態とした段階で，造船事業者により PT/TLPT を実施する。
③ 運用を開始したオンボードシステムと，当該システムの運用にかかわる組織の健全性を評価するために，船社によって定期的に TLPT を実施する。

今回の PT は上記②のタイミングを想定し，実施した。ただし，テスト環境の用意などの制約から，結果的には航海機

器系，機関系といった，単一機能を担保するシステムに対して，機能を評価する PT を行った。そのため，システム同士をインテグレートした際に生じうる脆弱性や，実運用時の設定の脆弱性，インシデントが発生してからの対応については検証できていない。

船舶のサイバーセキュリティは船舶航行の安全を担保するためであるという前提を踏まえると，特定船舶固有のリスクについて検証することが望ましい。2020 年 5 月に公表された IACS（国際船級協会連合）の Recommendation No.166 “Recommendation on Cyber Resilience”では，設計段階における検証に加えて，ネットワークケーブル及びすべてのデバイスの船舶への設置が完了した後にシステムが満足に機能することを確認するための試験が実施されるべきであることに言及している。

8. Verification Testing General The verification and testing should be carried out at different stages, such as Design verification, testing on board following installation and during ships life. Subsequent to construction of new builds the Vessel computer based system testing should be carried out to verify satisfactory performance of the system. The section specifies methodology to verify the requirements specified at section 7, as part of GBS approach. The testing should be carried out after complete installation of network cables and all devices. The simulation tests should demonstrate how the commands from the computer based system may be executed.	8. 検証試験 一般 検証及び試験は，設計の検証，設置後及び就航後の船上試験のように，異なる段階で実施されるべきである。船舶の建造後には，コンピュータベースのシステムが満足に機能することを確認するための試験が実施されるべきである。本セクションでは，GBS アプローチの一環として，セクション 7 に規定された要件を検証する方法を規定する。 試験は，ネットワークケーブル及びすべてのデバイスの設置が完了した後に実施されるべきである。シミュレーション試験は，コンピュータベースのシステムからのコマンドがどのように実行されるかを示すものであるべきである。

出所）http://www.iacs.org.uk/publications/recommendations/161-180/

以上のことに鑑みると，上記②のタイミングにおいて実施することが望ましい。ただし，②のタイミングで機器・システムの脆弱性が明らかになった場合，手戻りが非常に大きくなるか，手の施しようがない状態になってしまうため，舶用機器ベンダにおいては①の時点で PT を実施することが期待される。なお，ここで実施される PT は個別機器単位ではなく，型式単位での検証を想定する。また，造船事業者においては，型式単位で PT を実施した機器・システムを調達することが望ましい。

他方で，当然であるが，PT を実施する場合は開発コストや統合試験コストが増えることを意味する。そのため，船主においては，PT の実施を造船事業者に要求する場合には，当該コストも勘案した金額で発注したうえで，PT の実施を要求することが望ましい。

なお，PT を実施するタイミングが後になればなるほど，一回の試験で検証できる範囲は広くなる。①のタイミングでは機器・システムだけの検証だが，②のタイミングでは機器・システムを接続するネットワーク，③のタイミングでは運航後の設定や運用手順なども含めてテストできるからである。一方で，PT 実施タイミングが後になればなるほど，脆弱性を発見した場合の手戻りの手間は大きくなる。

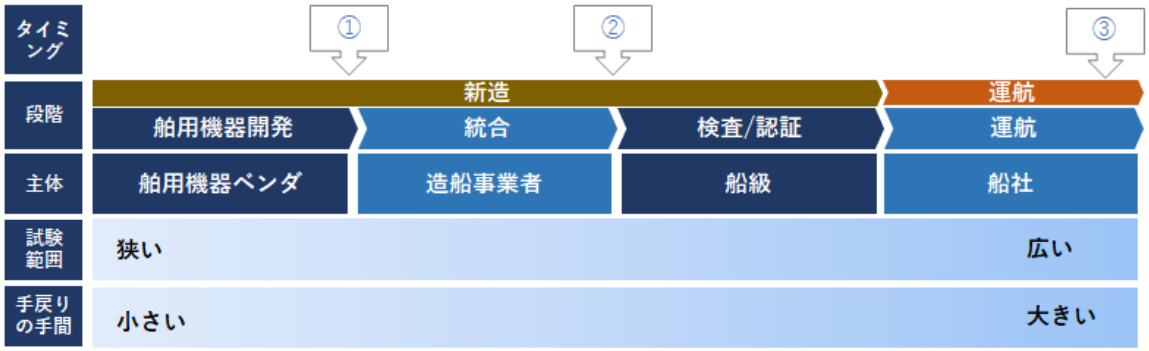


図 4.3.2　PT 実施タイミングと手戻りの手間・試験範囲の関係

②，③のタイミングで機器・システムの機能面での脆弱性を発見した場合，すでに統合が終了した機器・システムを改修する必要が生じる恐れがあるため，舶用機器開発段階及び統合段階におけるセキュリティ要件の確実な実装，運航段階におけるセキュリティ対策の継続的な運用管理に努める必要がある。

APPENDIX IoT セキュリティオーケストレーションエンジンの検証

A.1　　背景と目的

近年の技術革新により，物理やコストの制約により情報化されなかった従来デバイスにも演算処理，メモリ，他デバイスとの通信といった機能が実装され，それらを相互にネットワーク化することで，あらたな事業価値，社会価値の創造を試みる Internet of Things（以下，IoT）と呼ばれる世界が出現している。IoT の世界を構成する情報化されたデバイス（以下，IoT デバイス）には，その物理，コスト，使用環境等の制約からオフィス環境で用いる汎用パーソナルコンピュータや汎用サーバなどの機器とは異なる独自の設計仕様・実装仕様となっているものが多数存在する。このため，従来の汎用機器を前提としたセキュリティソリューションやセキュリティサービスを適用することが困難なユースケースが多数存在し，また特殊であればあるほどセキュリティベンダにとってビジネスのスケールが望めないがゆえに，ソリューションやサービスが市場に投入されにくいといった状況が出来している。汎用機器に比較してセキュリティ対策が遅れる傾向にあり，かつ，相応の計算資源を有しネットワーク化されている IoT デバイスがサイバー攻撃のターゲットとなることは当然の成り行きであり，大規模 IoT デバイスの乗っ取りと破壊，あるいは乗っ取った IoT デバイスを踏み台として特定のサービスを機能不全に陥れる DDoS 攻撃といったインシデント事例が多数知られているところである。

将来的には IoT の世界においても現在のオフィス環境と同程度のセキュリティ対策が講じられるようになるものと想定されるが，その順序としてユーザやセキュリティベンダにとってコスト面で比較的導入障壁の低い人手による運用対策，あるいは既存技術を比較的容易に転用できる技術対策が先行するものと思われる。IT セキュリティのノウハウを蓄積してきたセキュリティベンダの立場で眺めると，IoT デバイス間でやり取りされる TCP/IP 通信の監視と異常な通信の検知といった対策は，既存ノウハウを最も手軽に転用することができる対策の一つであり，TCP/IP 通信のみならず IoT デバイスの特殊な通信プロトコルもカバーするような通信監視・異常通信検知ソリューションも著名セキュリティベンダによって市場に投入されている。

一般的に，オフィス環境に通信監視・異常通信検知ソリューションを導入し，運用することはユーザにとって決して容易なことではない。オフィス環境における通信は非定型な通信先と非定型な通信を行うことが多く，正常通信と異常通信をどのように定義しても一定以上の誤検知が発生する。検知結果の真偽を判定するためには高度な専門性と相応の労力を要することが多く，セキュリティポリシーの設定や検知結果の真偽判定といった作業にはノウハウの蓄積が必要となる。一方，IoT デバイスによる通信はオフィス環境におけるそれと比較し，定型的であることが想定され，それゆえセキュリティポリシーの設定や誤検知の低減も比較的容易に行えるものと想定される。このことも IoT 世界をターゲットとした通信監視・異常通信検知ソリューションをセキュリティベンダが市場へ投入している理由のひとつと考えられる。

IoT セキュリティオーケストレーションエンジン（以下，ISE）は，このような文脈のなかで NTT セキュアプラットフォーム研究所（以下，NTT 研）により開発されたサイバー攻撃検知技術である。ISE は監視対象とするネットワークに接続する各ノード間で往来するレイヤー4 までの通信を観察し，事前に機械学習した正常通信との差異が閾値を超える，あるいは事前に学習したノード以外の不正に接続されたノードからの通信を発見すると，異常通信・不正機器接続として検知するとともに，異常と認定されたノード間の通信を自動的に遮断する機能を有しており，米国国立標準技術研究所（NIST）が提唱している Cyber Security Framework における「検知」と「対応」に呼応する技術となってい

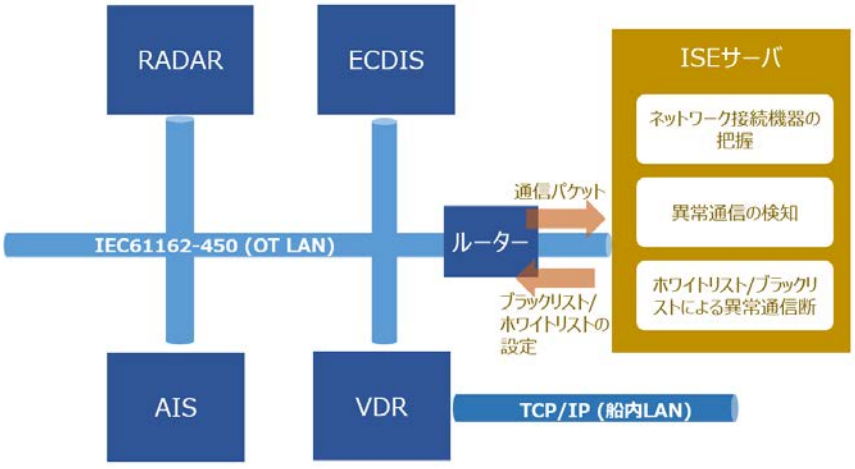


図 A.1.1　ISE のサービス

ISE をオンボードシステムに適用する場合，機器間を往来する通信が比較的定型的であり，かつ，第三者による不正アクセスによって海難事故等の重大インシデントにつながりやすい OT 系機器のレイヤー3 通信を監視対象とすることが想定される。ISE サーバはネットワーク上に設置されたルーターのミラーポートから通信パケットを取得し，通信断はルーターの設定変更によって行うため，既存ネットワークの構成を変更する必要がなく，通信パケットをリアルタイム（あるいは準リアルタイム）で観察できるのであれば，サーバを船内に設置する必要もない。仮に船陸間での低価格大容量高速通信が実現すれば，船上サーバ（ISO19847）経由で通信パケットを陸上のクラウド環境に設置している ISE サーバにリアルタイム転送し，陸上勤務の要員によるオンボードシステムのセキュリティ運用に活用するといったユースケースも想定される。

そこで本プロジェクトでは，前出の TLPT においてレッドチームによる疑似攻撃が行われている際の通信状態と疑似攻撃前の通信状態のコントラストが ISE によってどの程度明確にとらえられるのかという技術課題を検証するべく，本文 3.2 節に記載した TLPT 実施と並行して，ISE による異常通信検知実験を行うこととした。

A.2 ISE の概要

ISE サーバが提供する主な機能を表 A.2.1 に記載する。ISE は，処理の役割分担や負荷分散に対応するため，複数 ISE サーバによる処理連携や処理代行サーバとの処理連携に必要な機能も有している。

表 A.2.1 ISE の機能概要

主な機能	機能概要
①収集機能	機器解析・通信解析等で利用する情報(パケット情報・sFlow 情報)を収集し，不要な情報のフィルタを行い，利用可能(あるいは利用しやすい)データ形式への加工を行い，DB に保存する。
②機器解析機能	IoT 機器の通信パケットから解析に必要な情報を取得し，機械学習や機器解析補助用のスキャンツール等を動作させ，IoT 機器の機種を特定する。
③通信解析機能	ISE の管理対象の機器に対して正常通信モデルの生成を行い，異常通信の検知，異常検知通知の出力を行う機能である。ISE が機能として持つ「異常通信の検知」「不正機器接続の検知」を実現するための機能である。
④機器制御機能	通信解析機能や，GUI からの指示にもとづきホワイトリスト設定，ブラックリスト設定，機器隔離設定等の通信ルールをルーターに設定する機能である。また，定期処理にてドメイン変更追随，機器 IP 追随，機器削除追随を行い，必要に応じて通信ルールの再設定を行う。
⑤自律連携機能	自律連携機能は，大きく分けて以下の2種類の機能を有する。 ● シグネチャ共有：ISE が機器解析，通信解析の処理を行う際に，他の ISE での解析結果を自動的に受信，あるいは解析結果を他の ISE へ自動的に送信する機能である。 ● サーバ連携：ISE が他の ISE にデータを送信することによって，処理の委譲による負荷軽減や保守情報の集約化を実現するための機能である。
⑥データフロー制御機能	各機能の起動および機能間のデータ受け渡しの仲介を行う機能である。

ISE による通信解析は，機械学習によって正常通信モデルを生成（正常通信状態を学習）し，当該モデルとの比較によって異常通信の検出を実現している。また，機器解析機能により特定された機種ごとに正常通信の通信先を学習すること及び通信パケットより通信元を取得することにより，不正機器接続の検知を実現している。ISE では信頼区間分析，主成分分析，ホワイトリスト学習の３法を組み合わせた正常通信モデルの生成を行っている。

表 A.2.2　ISE における学習手法

手法	概要
信頼区間分析	5 分間毎に集計される統計値を利用した学習アルゴリズム。統計値には宛先 IP 数・宛先ポート数・パケット送受信比等全 22 種存在しており，それぞれの統計種別から信頼できる値の上限値を算出する。
主成分分析	5 分間毎に集計される統計値を利用した学習アルゴリズム。統計値から機器の相関関係を学習し，統計値から相関関係から外れた通信が発生した場合に異常として判定を行う。
ホワイトリスト学習	正常通信学習期間内に含まれる宛先を蓄積し，ある程度の飽和状態となった場合に学習完了としてホワイトリストを作成する。

A.3　技術検証における前提・制約

本検証では，本文 3.2 節に記載した被験システムのネットワークにおいて発生する正常通信を学習し，レッドチームによる疑似攻撃で発生する通信（異常通信），及びレッドチームの機器の接続(不正機器接続)を識別する。本来，ISE が観察する対象は運航中の船舶におけるオンボードシステムの通信であり，乗員や陸上設備要員による業務遂行，接続している他システムでの処理，機器故障といったイベントによって通信状態が変化することが想定されるが，本検証ではそれらの通信状態を再現しないこととしている。

疑似攻撃で発生する通信を ISE が識別できたかどうかを検証するためには，レッドチームが通信を伴うアクション（たとえば，ある IP アドレスを有する機器のあるサービスポートに向けてなんらかのリクエストコマンドを送信する，などのアクションを単位アクションとする）を実行していたかどうかを単位アクションごとに把握する必要があるが，レッドチームのアクションは PT プロバイダのビジネスノウハウであり，その開示は限定的となる。従って，ISE の識別能力の判定に際し，通信が発生するかどうかについて PT プロバイダより開示を受けることができなかったレッドチームのアクションについては，ISE の識別能力の判定の材料に含めないこととする。

前述のように ISE には異常を検知した際にセキュリティポリシーに従い，ネットワークルータの機能を利用して通信断を実行する機能が具備されているが，今回の被験システムにはそのようなネットワークルータが含まれていないため，通信断に関する検証は対象外としている。

今回は異常通信の識別性能の検証にのみフォーカスし，ISE のリアルタイム処理性能に関する検証は行わない。

A.4　古野電気実験環境における評価の概要

実施期間および実施環境

実施期間：

2019 年 12 月 6 日，7 日，8 日，9 日（正常通信パケット収集期間）

2019 年 12 月 9 日，10 日，11 日（疑似攻撃時の通信パケット収集期間）

被験システム設営場所；

古野電気（株）東京支社

〒101-0024 東京都千代田区神田和泉町 2-6 今川ビル

被験システム構成機器：

FMD-3200(ECDIS)

VR-7000(VDR)

GP-170(GPS)

TG-8000(GYRO COMPASS)

Repeater Hub

Packet Sniffer（NTT 研持ち込み機材）

検証の段取り

本文図 3.1.2 の OT LAN に接続する Repeater Hub に通信パケット取集機器（Packet Sniffer）を結線し，疑似攻撃着手前および疑似攻撃着手後に OT LAN を往来する通信パケットをそれぞれ取集する。その後，パケット再送ツールを用い，別環境で通信状態を再現したうえで正常通信状態の学習および異常通信の検知，不正機器接続の検知を行う。経験上，正常状態の学習には 1 週間程度の正常通信状態を再現し，学習することが望ましいが，本検証では正常通信状態の再現については 68 時間が上限となったため，68 時間分の正常通信状態を無制限の繰り返し学習を行うことで学習データの不足を補完することとしている。

正常通信状態の学習

主成分学習とホワイトリスト学習においては被験システムの構成機器に関する学習を全て完了した段階で，信頼区間学習においては統計種別ごとの学習が完了した段階で，ISE による正常通信状態に関する学習が完了したとみなしている。信頼区間学習では「値が連続していない」統計種別は学習不可であるため，再学習等は実施しないこととしている。ISE では正常通信学習期間中に学習が収束せず，学習モデルを得られない事態が出来することがある。この「学習モデル不可状態」を回避する為，いくつかの学習条件を緩和した設定パターンを作成し，学習を行っている。学習パラメータを表 A.4.1 に示す。下表 A.4.1 のオレンジ色網掛け項目が，学習条件を緩和したパターンである。

表 A.4.1 学習パラメータの設定

設定区分	各パラメータ	設定値
学習期間設定	初期値(時)	24
	上限値(時)	96
	下限値(時)	6
	変更係数	1.5
検証期間設定	初期値(時)	6
	上限値(時)	96
	下限値(時)	6
	算出係数	1.5
主成分モデル設定	自動連携依頼基準(秒)	60
	同時学習機器数	20
信頼区間モデル設定	モデル適用期間(時)	120
	信頼水準	0.999
	同時学習機器数	20
	信頼区間近似曲線種別	1
	信頼区間学習履歴データ件数下限	5
	信頼区間学習完了勾配	0.4
	信頼区間学習履歴データ件数上限	720
	信頼区間学習対象外経過時間(分)	60
	信頼区間学習収束予測値最低必要数	5
	信頼区間学習収束予測値最大誤差割合	0.25

検証結果

古野電気実験環境の TLPT において，ISE は接続された 3 台のレッドチームの機器のうち，3 台すべてを検出することができた。

同環境の TLPT において，ISE は計 631 件の通信異常を発報した。当該発報履歴とレッドチームの作業履歴を突合したところ，OT LAN 上にレッドチーム由来の通信を発生させると想定される 19 単位アクションについては，計 19 件の発報として 631 件の発報に含まれていた。ISE は学習したモデルとの差異を認識するエンジンであり，その出力には発報の原因（発報を誘発する攻撃者のアクション）を特定するための情報を含むものではない。実際，ISE による 19 件の発報のなかで，レッドチームの作業履歴を突合させても原因を一意に特定できない例として以下を示す。

- ある時刻に ISE が宛先ポート数の増加という事象を捉えたが，当該時刻にレッドチームが ECDIS に対してポートスキャンと脆弱性スキャンを同時に実施していた。アウトバウンドのみを監視する ISE はどちらのスキャンも宛先ポート数の増加という事象として検知するため，どちらの行為に起因する現象であるかを識別することができない。
- ある時刻に学習期間において発生しなかった HTTP 通信の発生を ISE が捉え発報したが，同時刻にレッドチームが ECDIS の Web 画面に対して脆弱性スキャンを実行していた。ISE は HTTP 通信の発生のみを検知するため，それがどのような行為に起因する現象であるかを識別することができない。
- 5 分未満の時刻幅において，監視対象機器に対するポートスキャンおよび rsync による接続試行によって発生した通信を ISE が捉え発報したが，ISE の信頼区間学習・主成分分析では 5 分ごとの統計情報が揃ったタイミングで学習モデルと比較を実施しており，ISE による発報がどちらの行為に起因する現象であるかを識別することができない。

なお，全発報件数 631 件から上記 19 件の発報を除く 612 件の発報については，その偽判定の割合を特定することができていない。これは，レッドチームによって開示される作業履歴の粒度が偽判定の分析に不十分であること，また，粒度の高い作業履歴は PT プロバイダのビジネスノウハウに該当するため，ISE の評価者に当該履歴が開示されなかったことによる。

A.5　　日本無線実験環境における評価の概要

実施期間および実施環境

実施期間：

2020 年 1 月 10 日～14 日（正常通信パケット収集期間）

2020 年 1 月 8 日，9 日，10 日（疑似攻撃時の通信パケット収集期間）

被験システム設営場所：

日本無線（株）辰巳事業所

〒135-0053　東京都江東区辰巳 1-7-32

被験システム構成機器：

JAN-9201(ECDIS)

JCY-1900(VDR)

JLR-8600(GPS)

JMR-9200(RADAR)

JHS-183(AIS)

Repeater Hub

Packet Sniffer（NTT 研持ち込み機材）

検証の段取り

本文図 3.1.2 の OT LAN に接続する Repeater Hub に通信パケット取集機器（Packet Sniffer）を結線し，疑似攻撃着手前および疑似攻撃着手後に OT LAN を往来する通信パケットをそれぞれ取集する。その後，パケット再送ツールを用い，別環境で通信状態を再現したうえで正常通信状態の学習および異常通信の検知，不正機器接続の検知を行う。経験上，正常状態の学習には 1 週間程度の正常通信状態を再現し，学習することが望ましいが，本検証では正常通信状態の再現につ

いては 91 時間が上限となったため，91 時間分の正常通信状態を無制限の繰り返し学習を行うことで学習データの不足を補完することとしている。本検証では，正常通信学習期間はおよそ 91 時間分取得したが，ISE の学習期間としては不十分な可能性が高いためパケット再送ツールによりループすることで対応した。ループには回数を指定せず，無制限でループを実施した。

正常通信状態の学習

ホワイトリスト学習においては被験システムの構成機器に関する学習を全て完了した段階で，信頼区間学習においては統計種別ごとの学習が完了した段階で，ISE による正常通信状態に関する学習が完了したとみなしている。信頼区間学習では「値が連続していない」統計種別は学習不可であるため，再学習等は実施しないこととしている。主成分学習では学習モデルの作成が完了できなかったため，5 機器中 1 機器のみ学習完了，4 機器が検証期間中の状態で，異常通信検知の検証を実施した。これは所与の学習時間では主成分学習を終了できなかったためであるが，これにより主成分分析による異常検知が機能しない場合が出来することを許容することとした。ISE では正常通信学習期間中に学習が収束せず，学習モデルを得られない事態が出来することがある。この「学習モデル不可状態」を回避する為，いくつかの学習条件を緩和した設定パターンを作成し，学習を行っている。学習パラメータを表 A.5.1 に示す。下表 A.5.1 のオレンジ色網掛け項目が，学習条件を緩和したパターンである。

表 A.5.1 学習パラメータの設定

設定区分	各パラメータ	設定値
学習期間設定	初期値(時)	24
	上限値(時)	300
	下限値(時)	6
	変更係数	1.5
検証期間設定	初期値(時)	6
	上限値(時)	300
	下限値(時)	6
	算出係数	1.5
主成分モデル設定	自動連携依頼基準(秒)	60
	同時学習機器数	20
信頼区間モデル設定	モデル適用期間(時)	360
	信頼水準	0.999
	同時学習機器数	20
	信頼区間近似曲線種別	1
	信頼区間学習履歴データ件数下限	5
	信頼区間学習完了勾配	0.4
	信頼区間学習履歴データ件数上限	720
	信頼区間学習対象外経過時間(分)	60
	信頼区間学習収束予測値最低必要数	5
	信頼区間学習収束予測値最大誤差割合	0.25

検証結果

日本無線実験環境の TLPT において，ISE は接続された 2 台のレッドチームの機器のうち，2 台すべてを検出することができた。

同環境の TLPT において，ISE は計 10,331 件の通信異常を発報した。当該発報履歴とレッドチームの作業履歴を突合したところ，OT LAN 上にレッドチーム由来の通信を発生させると想定される 18 単位アクションについては 18 件の発報として 1,0331 件の発報に含まれていた。なお，18 件の発報には A.4 節に記載した理由などにより，レッドチームの作業履歴と突合させても原因を一意に特定できないケースが 6 件含まれていた。全発報件数 10,331 件から上記 18 件の発報を除

く 10,313 件の発報については，その偽判定の割合を特定することができていない。これは，レッドチームによって開示される作業履歴の粒度が偽判定の分析に不十分であること，また，粒度の高い作業履歴は PT プロバイダのビジネスノウハウに該当するため，ISE の評価者に当該履歴が開示されなかったことによる。

A.6 Future work

レッドチームの作業履歴から異常通信を発生させるであろうレッドチームアクションを抽出し，同時刻における ISE の発報履歴を突合させたところ，抽出されたすべてのアクションに対して ISE が発報していたことを確認した。一方で，当該技術の有効性を結論づけるためには，真偽不明の発報(古野電気実験環境では 600 件程度，日本無線実験環境では 10,000 件程度)のうちどの程度が誤検知に該当する（レッドチームアクションに起因しない）発報であるのかを検証することが必要である。誤検知の頻発は運用者による要因の切り分け作業負荷を増大させるほか，システムの可用性を確保するためにセキュリティポリシーを緩めざるを得なくなり，結果としてサイバー攻撃を検知できないという状況を出来させる。PT プロバイダのノウハウ開示を受けることで，誤検知の切り分けとより詳細な分析を行い，ISE の有効性をよりよく検討することが可能となる。

また，今回の検証はあくまで実験環境における検証であり，外洋航海中の乗員による作業で発生するであろう通信を再現していない。人手作業を起因とする通信が頻発するオフィス環境では一般的に誤検知が一定以上発生することが避けられず，可用性を確保するために誤検知を避けようとすれば，検知漏れ事象が増大するというトレードオフの関係が存在する。外洋航海中の作業に伴い発生する通信を正常通信として ISE に学習させた場合，それらの通信が非定型で一定以上の頻度で発生するならば，サイバー攻撃に起因する異常通信を正常な通信と誤認識する状況が出来することも十分想定できる。ISE が真に有用な技術であることを示すためには，より実際的な環境において，誤検知や検知漏れに関するより詳細な検証が必要となる。

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

一般財団法人 日本海事協会 海技部

〒102-0094 東京都千代田区紀尾井町 4 番 7 号
Tel: 03-5226-2177
Fax: 03-5226-2013
E-mail: met@classnk.or.jp

www.classnk.or.jp

July 2020