

海事サイバーセキュリティセミナー2025

海事サイバーセキュリティセミナーは、広島商船高等専門学校を中心に、日本財団の支援を受けて始動した海事サイバーセキュリティ人材育成プロジェクトの一環として開催されました。

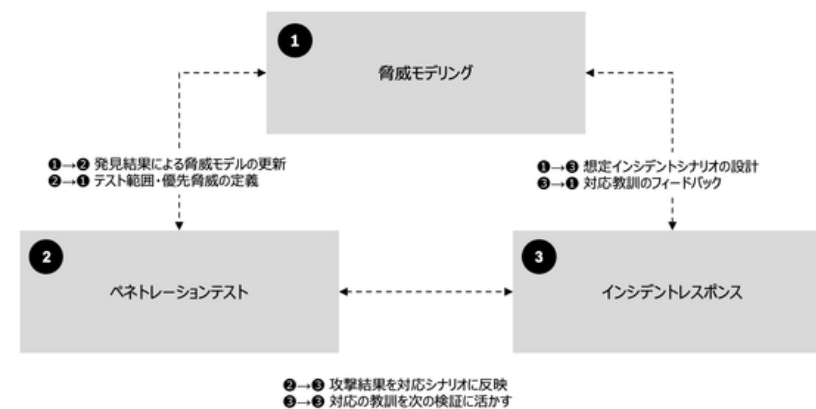
セミナーの目的

- ①船舶に関わるサイバー攻撃の脅威や、考え得るサイバーセキュリティ対策について議論および体験する場を提供する
- ②会員企業の参加者同士の交流、高等専門学校の情報系並びに、商船学科の教員及び学生との交流を図る

オンラインでの事前学習と、広島県にある広島商船高専および練習船「広島丸」での現地開催を組み合わせた複数日程で実施しました。

3つの実践演習

本セミナーは、脅威モデリング・ペネトレーションテスト・インシデントレスポンスの3つの演習を通じて、攻撃から防御、対応までを一貫して体験できる実践型プログラムです。



脅威モデリング

システムや機器に対する脅威（攻撃者・攻撃手法）を洗い出し、リスクを体系的に特定・分析するリスク評価手法



ペネトレーションテスト

システムや機器について洗い出した脅威に対して、リスクが存在するか実際に攻撃を試み、脆弱性やセキュリティの強度を調査するテスト手法



インシデントレスポンス

発生したインシデントに対処し、それらの影響を軽減し、学んだ教訓に基づいて、インシデントレスポンスとマネジメントの実践を確立・改善するための手法

海の現場にもサイバーセキュリティが必要な時代。

Our Mission

海事分野のデジタル化・自動化の進展に伴い、航行停止や港湾機能の麻痺、情報漏えい等の重大リスクが顕在化しています。安定的な海上輸送を守るには、機器対策に加え、現場で迅速に判断・対応できる人材が不可欠です。本プロジェクトは産官学連携の実践的学習を通じ、海の安全と持続的発展を支えるサイバー人材の育成を目指しています。

本プロジェクトは、広島商船高等専門学校を中心に、日本財団や海事関連業界の協力のもと進められている、産官学連携の取り組みです。運営には、広島商船高専の教職員に加え、サイバーセキュリティ企業や、人材育成、教育業界のプロフェッショナルたちが参加し、専門性を活かしながら連携しています。

プロジェクトの取り組みをnoteで発信しています



日本財団助成事業
MEGURI2040を支える船舶の高度な自動化を開発運用できる人材育成プロジェクト

開催報告

海事サイバーセキュリティセミナー 2025

関係校
広島商船・高知・木更津・一関・仙台・富山・石川
・鳥羽商船・大島商船・新居浜・弓削商船

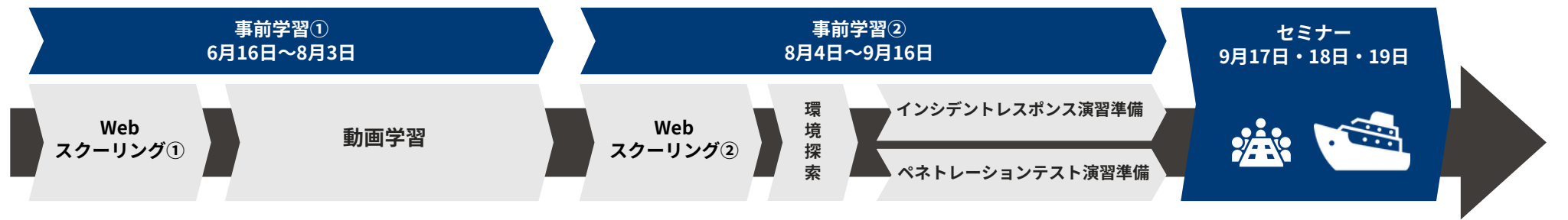
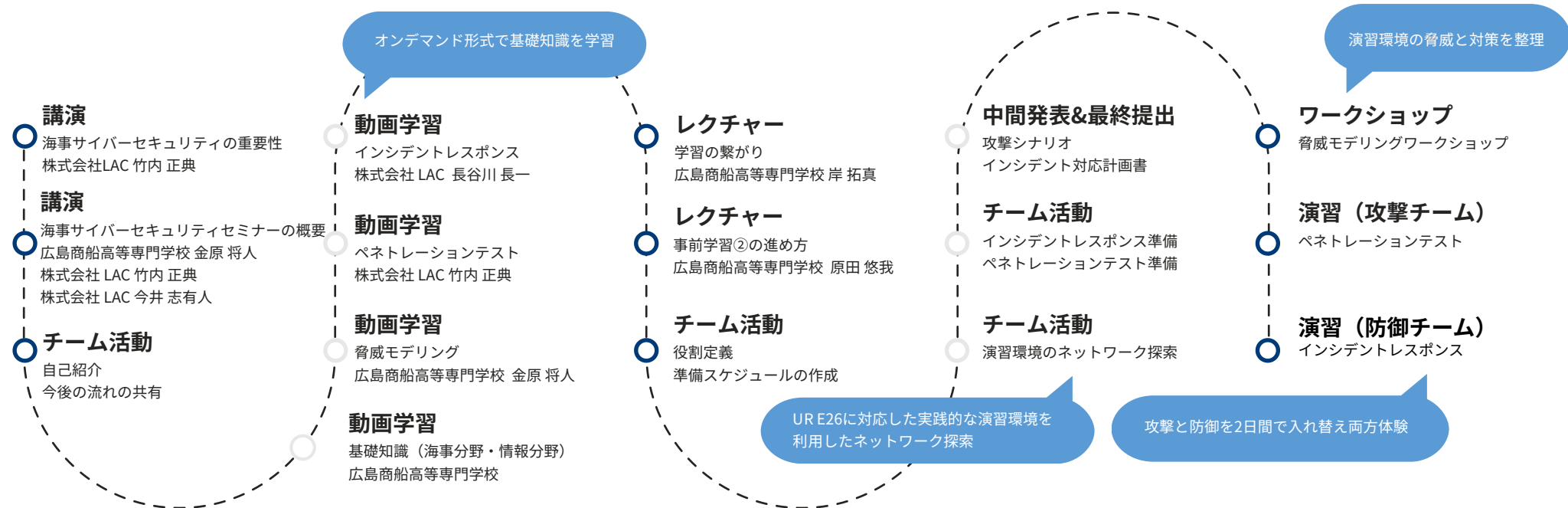
後援
竹原市・大崎上島町
一般社団法人日本船用工業会

協力
株式会社ラック



- ① 船舶に関わるサイバー攻撃の脅威および想定されるサイバーセキュリティ対策について、議論ならびに体験の機会を提供する。
- ② 本セミナーを通じ、会員企業の参加者間の交流を促進するとともに、高等専門学校（情報系および商船学科）の教員・学生との交流を図る。

セミナー

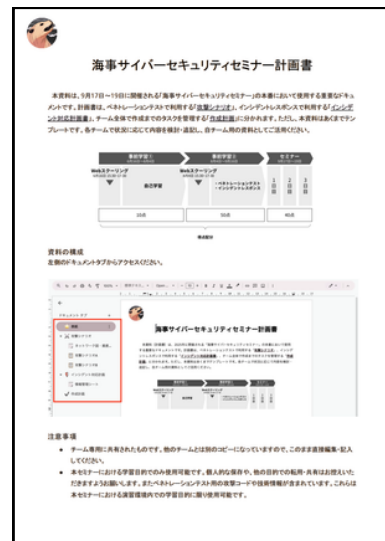


各演習に必要な事前の知識を習得するために、基礎知識（海事）・基礎知識（IT）・脅威モデリング・インシデントレスポンス・ペネトレーションテストのオンデマンド教材を学習。オンデマンド教材は事前学習①の期間外も提供し、各自のタイミングで繰り返し学習ができるようにしています。



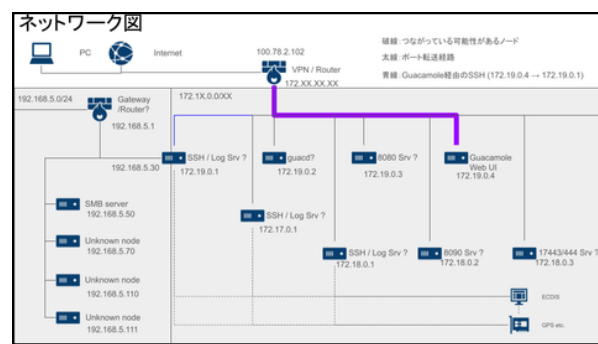
Webスクーリング①の様子

動画学習の様子

[illegible]

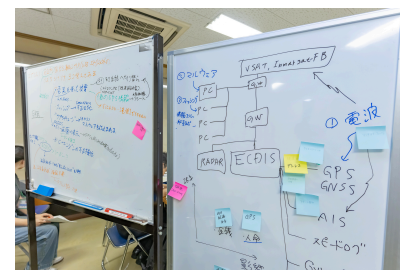
計画書

演習環境にアクセスした上でネットワーク探索を実施。その後、チームでペネトレーションテストで利用する「攻撃シナリオ」、インシデントレスポンスで利用する「インシデント対応計画書」の作成を行いました。

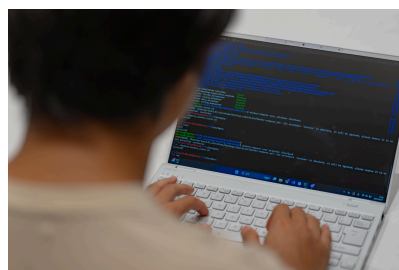
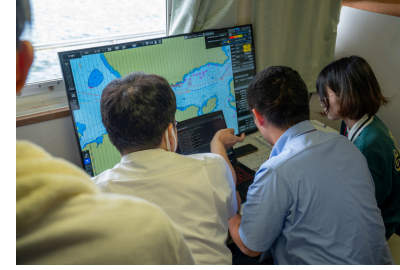


受講生が作成したネットワーク図

システムを俯瞰して眺め、「どこにリスクが潜んでいるか」をチームで考えるワークショップです。専門家のサポートのもと、チームで図を描きながら脅威を洗い出し整理。限られた時間で意見を出し合い、リスクを可視化する過程を体験します。



実際に演習用のネットワークに攻撃を試みて検証する実践セッションです。事前学習で学んだことをベースに攻撃手法を体感。机上ではなく「やってみて理解する」ことで、脆弱性評価のリアリティを学びます。



事前に作成した計画書をもとに、発生したサイバー攻撃への対応をチームで実施する演習です。どの情報を優先して共有し、どの順に復旧するかを議論。対応を振り返りながら、危機時の意思決定や連携の重要性を実感します。

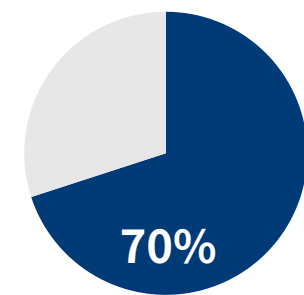


成果 ※1

日本船用工業会会員

得られて良かった内容

満足度



1位	リスク認識やインシデント対応に関する実践的な学び
2位	サイバーセキュリティ対策に対する必要性の理解
3位	実務に役立つ知識やスキルの習得
	実際の船を使った演習でリアルな感覚の体験
	他の参加者（社会人）との交流
	規格や標準を業務に落とし込むヒント



一般社員

自分の知識不足を感じました。また、インシデントレスポンスにあたり、正解はなく、柔軟な思考も重要であると学ぶことができました。難しかったですが、楽しかったです！
来年参加してリベンジしたいです。



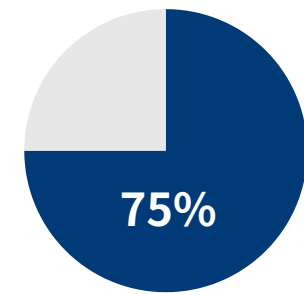
セキュリティ担当

脅威モデリング、ペネトレーションテスト、インシデントレスポンスの3つ全ての項目において、知識をつけていく事前学習だけでなく、それを活かす演習があることが総復習となって、経験として身につく学習ができたと感じます。

高等専門学校学生

得られて良かった内容

満足度



1位	実際の船を使った演習でリアルな感覚の体験
2位	実務に役立つ知識やスキルの習得
	リスク認識やインシデント対応に関する実践的な学び
	サイバーセキュリティ対策の全体像の理解
5位	他の参加者（社会人）との交流



商船系学生

私は操船の役割をしていました。ECDISに頼る航海をいつも通り行っていたので、ECDIS画面が真っ白になった時はとても戸惑った。新しい知識や、将来乗船中に実際に攻撃を受けた場合の動き方を経験として学ぶことが出来、とても有意義で楽しい3日間になりました。



情報系学生

脅威モデリングとインシデントレスポンスで実際に現場でインシデントが起きた際の対応を経験し、ペネトレーションテストで攻撃側も体験したことで、脆弱性の危険さを理解し、対応のための事前準備の重要性を実感することができました。

※1セミナー終了時に参加者を対象に実施したアンケート調査。満足度は「海事サイバーセキュリティセミナーの満足度についてお聞かせください」という設問に対して、6段階評価のうち「6」もしくは「5」をつけた参加者の割合。得られて良かった内容は「最も得られてよかったことを1つ選択ください。」という設問に対して最も回答の多かった内容