別添資料：e ラーニング 2026 年版コンテンツ

①　はじめての海運・造船講座（2026 年版）
受講料：10,000 円（税別）/人
標準学習時間：計 2 時間程度
受講対象者：海事産業に初めて従事する新入社員、内定者など
章構成：
1. 海事産業の基礎知識
2. 海運・造船ビジネスの基礎
3. 様々な貨物船
4. 建造工程
5. 船舶の設備 1
6. 船舶の設備 2
7. 船舶に適用される法規
8. 船舶の性能

概要：
船舶・造船を冠した学部/学科の減少により、以前にも増して新入社員への基礎教育の必要性が高まる一方、習得すべき知識は増加し、新人教育はますます複雑化しています。そのため、はじめて海運・造船業界に関わる方が業務に携わる上で有用な知識を、分かりやすく丁寧に解説することを目的とした e ラーニング講座を提供しています。今年度版では各種データの最新化等のアップデートを行っています。

②　そのつぎの海運・造船講座　復原性編（2026 年版）
受講料：10,000 円（税別）/人
標準学習時間：計 1 時間程度
受講対象者：造船所などの若手設計者
章構成：
1. 船舶が転覆しない仕組み
2. 船舶は損傷しても転覆しないのか？

概要：
船の海難事故がひとたび起こると、人命・財産の喪失ばかりでなく、海洋環境に大きな損害を与えます。この海難事故を防止し、損害の最小化を図るため、新造船には復原性に関する規則が適用されます。本講座では、これから船の計画、設計あるいは運航に関わる方を主な対象に、船に働く浮力

や復原力の発生原理から非損傷時及び損傷時復原性規則の内容に至るまで、船の復原性に関わる基本的な知識を、動画やアニメーションなどを使って分かりやすく解説します。

③　そのつぎの海運・造船講座　船型設計編（2026 年版）
受講料：10,000 円（税別）/人
標準学習時間：計 1.5 時間程度
受講対象者：造船所などの若手設計者
章構成：
1. 船舶の推進と効率
2. 船体抵抗と性能設計
3. 性能設計の手法とツール

概要：
海事産業では、GHG 排出削減が緊急の課題として大きな注目を集めています。そのためのキーテクノロジーの一つが船の推進性能向上技術ですが、非常に専門性が高く理解が難しい技術でもあります。本講座では、造船技術者のみならず、船舶の性能に関する知識を必要とする方を対象に、プロペラの原理から船型や省エネ付加物の性能に及ぼす影響に至るまで、船型設計に関する幅広い知識を、水槽試験や数値流体力学（CFD）の動画などを使って分かりやすく解説します。

④　そのつぎの海運・造船講座　船体構造・強度編（2026 年版）
受講料：20,000 円（税別）/人
標準学習時間：計 2.5 時間程度
受講対象者：造船所などの設計技術者、建造監督等の若手技術者
章構成：
1. 船が壊れない仕組み
2. 船に働く力（荷重と応答）
3. 船が耐える力（強度）
4. 船が壊れないための評価
5. 船級協会の社会的責任

概要：
船は、大量の貨物を荒れた海域においても安全に輸送するために造られた巨大な構造物です。この構造物を設計し、建造するためには多くの知識と経験が必要となります。本会が提供する e ラーニング講座では、設計技術者、建造監督等の若手技術者を主な対象に、船が壊れない仕組みから、強度評価において必要となる荷重や構造応答についての基本的な知識まで、動画やアニメーションを

使ってわかりやすく解説します。また、船体損傷に関する統計といくつかの事例を紹介するとともに、船体損傷を減少させるために行っている船級協会の取り組みについても紹介します。

さらに、以下のコースを今後順次公開予定です。

⑤　海事サイバーセキュリティ 船上基礎コース –船員向け–
受講料：10,000 円(税別)/人
標準学習時間：約 30 分
受講対象者（目安）：船員
章構成：
1. サイバー攻撃について
2. 電子メールの安全な利用方法
3. クラウドサービスの安全な利用方法
4. 個人所有デバイスの安全な利用方法
5. ID・パスワードの安全な利用方法
6. USB メモリ等(外部記憶媒体)の安全な利用方法

概要：
船舶の"スマート化"が進み、海事産業の更なる発展が期待される一方、サイバー攻撃によるシステムへの不正侵入、情報漏洩、データ改ざんといったリスクもそれに伴って増加しております。こうした状況の下、日頃より船舶の運航に携わられている船員、海運会社並びにその他海事産業従事者におかれましては、サイバーセキュリティに関する正しい知識を身に着けていただくことが、本船システムへのサイバー攻撃を防ぐための第一歩となります。本講座では、外航、内航を問わず、船員様が知っておくべき基本的なサイバーセキュリティ対応について紹介します。

⑥　海事サイバーセキュリティ 船上上級コース –管理者向け–
受講料：15,000 円(税別)/人
標準学習時間：約 1 時間（各言語）
受講対象者（目安）：船上の IT システムを管理する方
章構成：
1. サイバー攻撃について
2. 電子メールの安全な利用方法
3. クラウドサービスの安全な利用方法
4. 個人所有デバイスの安全な利用方法

5. ID・パスワードの安全な利用方法
6. USB メモリ等(外部記憶媒体)の安全な利用方法
7. マルウェアについての理解
8. サイバー攻撃の兆候についての理解
9. アップグレードとソフトウェアメンテナンスについての理解
10. リモートアクセスのセキュリティについての理解
11. 管理者権限についての理解
12. 内部不正行為についての理解と対策
13. データ消去を含む使用済み機器の廃棄方法についての理解

概要：

船舶の"スマート化"が進み、海事産業の更なる発展が期待される一方、サイバー攻撃によるシステムへの不正侵入、情報漏洩、データ改ざんといったリスクもそれに伴って増加しております。こうした状況の下、日頃より船舶の運航に携わられている船員、海運会社並びにその他海事産業従事者におかれましては、サイバーセキュリティに関する正しい知識を身に着けていただくことが、本船システムへのサイバー攻撃を防ぐための第一歩となります。

本講座では、船員の IT 環境及び、サイバーセキュリティを管理する船上管理者様が知っておくべきサイバーセキュリティ対応について紹介します。

注：「海事サイバーセキュリティ 船上基礎コース –船員向け–」の全学習内容が含まれており、プラスアルファで船上管理者向けの学習内容が追加されたコンテンツとなります。

⑦ 海事サイバーセキュリティコース –CSMS 構築–

受講料：10,000 円（税別）/人

標準学習時間：約 1 時間

受講対象者(目安)：サイバーセキュリティマネジメントシステム構築に関わる方

章構成：

1. サイバーセキュリティマネジメントシステム構築の概要
2. NK サイバーセキュリティマネジメントシステムの要求事項
3. 会社及び船舶において実施するサイバーセキュリティ管理策
4. OCIMF VIQ、TMSA におけるサイバーセキュリティ

概要：

船舶の"スマート化"が進み、海事産業の更なる発展が期待される一方、サイバー攻撃によるシステムへの不正侵入、情報漏洩、データ改ざんといったリスクもそれに伴って増加しております。こうした状況の下、国際安全管理（ISM）コードの目的及び機能的要件に従って、サイバーセキュリティマネジメントシス

テムを安全管理システムにおいて考慮されることが推奨されています。本講座では、弊会が発行したガイドライン「船舶におけるサイバーセキュリティマネジメントシステム」に準拠して、船舶管理会社が構築するサイバーセキュリティマネジメントシステムについて解説します。

⑧　海事サイバーセキュリティ技術コース –サイバー攻撃対策編–
受講料：10,000 円（税別）/人
標準学習時間：約 1 時間
受講対象者(目安)：会社の IT システムを管理する方
章構成：
1. サイバー攻撃について
2. マルウェアについての理解
3. 標的型メール攻撃について
4. 内部不正についての理解
5. ランサムウェア
6. IoT 機器の不正利用について

概要：
船舶の"スマート化"が進み、海事産業の更なる発展が期待される一方、サイバー攻撃によるシステムへの不正侵入、情報漏洩、データ改ざんといったリスクもそれに伴って増加しております。こうした状況の下、日頃より船舶の運航に携わられている船員、海運会社並びにその他海事産業従事者におかれましては、サイバーセキュリティに関する正しい知識を身に着けていただくことが、本船システムへのサイバー攻撃を防ぐための第一歩となります。
本講座では、実際に海事産業において発生したインシデント事例、攻撃手法ならびにその対策法について解説します。

以上