海事保安に係るリスク評価

太田　進

Evaluation of Maritime Security Risk

by

Susumu OTA

1　はじめに

海事保安に係るリスク評価について述べるにあたり、戦争や暴力行為による船舶の被害の発生頻度を、衝突や火災と言った事故のそれと比較してみた。ロイド船舶事故データ [1] に基づく事故種別（Casualty Category）毎の件数を図 1 に示す。ここで、ロイド船舶事故データは、船舶に一定程度以上の損傷が発生した事例のみを収録しており、船舶の損傷を伴わない乗船者の死傷事例等は収録されていない可能性がある点に留意されたい。「件数」は一つの指標であり、当該事象の重要性を代表するものではないが、図より、「戦闘行為等」の件数は、全体の 1.5 %程度であることが分かる。以下、海事保安に係るリスクとその評価方法について述べる。

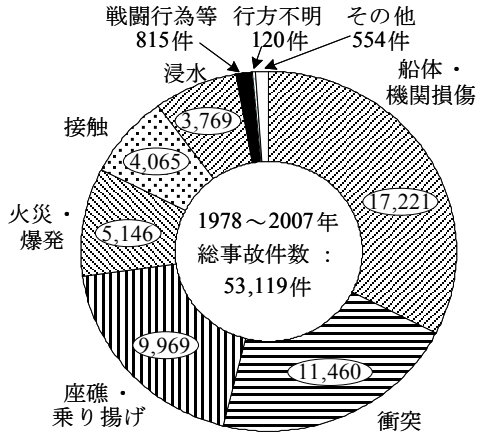

図 1　事故種別毎の件数

2　リスクの定義

一般に、保安、即ちテロや各種犯罪によるリスクは、安全上のリスクの一部として評価される [2]。そこでまず、安全上のリスク評価に倣って「船舶が保有する乗船者の生命に関するリスク」を考える。図 2 は、前述のロイド船舶事故データに基づき、事故種別毎の死者数及び行方不明者数の合計を示したものである。図より、戦闘行為等による死者及び行方不明者の数は、全体の 5 %程度であることが分かる。しかし、保安対策の重要性は、こうした定義のリスクのみでは評価できない。

保安に係るリスクを船舶の安全上の問題として評価する場合には前述の定義を用いるのが一般的であろうが、例えば新たに危険物ばら積み船用のターミナルを建設するといった場合には、「当該ターミナルの運用が保有する地域の人命／環境に関するリスク」が評価されるのが一般的である。この場合テロは、通常の事故と比較して、「被害規模の大きいシナリオ」に繋がる脅威／危険性となる可能性がある。

海事保安に係るもう一つの観点は「船舶等がテロ等の手段となる」または「テロ等の手段となる武器等、特に大量破壊兵器の運搬に利用される」

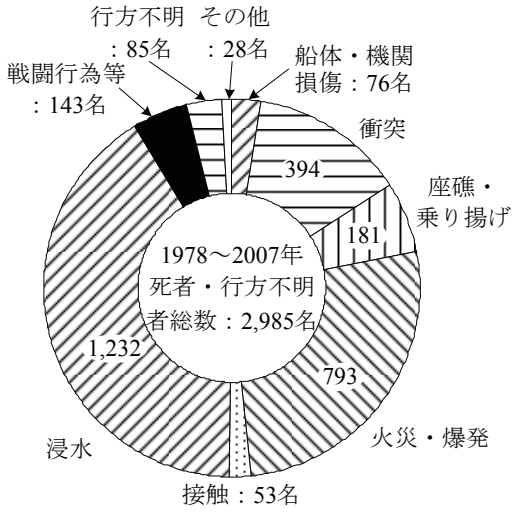

図 2　事故種別毎の死者・行方不明者の数

ことである。こうした事象を考慮して保安対策を評価するには、例えば「船舶運航を含む経済・社会活動が保有する国／世界の人命に関するリスク」を検討するのが適当かもしれない。しかしながら、いわゆるサプライチェーンセキュリティーの分野では、「保安について評価・対策・管理が実施されているか否か」、即ち、保安に係る取り組みがなされているか否かが問われるだけで、各種保安対策の効果を定量的に論じるには至っていない。即ち、こうしたリスクの評価については、まだ十分に研究されていないと言える。

3　国際船舶港湾施設保安法

2001 年 9 月 11 日の同時多発テロ事件以来、海事分野においても保安対策の強化が求められるようになり、国際海事機関においても様々な検討がなされてきた。その結果、SOLAS 条約付属書に新たに第 XI-2 章 [3]が追加され、また、この新章によって International Ship and Port Facility Security (ISPS) Code[4]が強制化され、2004 年 7 月 1 日に発効した。これを受けて我が国では、国際船舶港湾施設保安法等 [5]が制定された。ISPS Code では、説明の目的で Risk という言葉が用いられ、また、Security risk という言葉も用いられているが、保安計画策定の基礎となる危険性の評価は "Security Assessment" と呼ばれている。これに倣って、以下、ISPS Code で要求される保安上の危険性の評価を「保安評価」と呼ぶ。また、説明の都合上、通常の事故による危険性の評価を「安全評価」と呼ぶ。

保安評価には、船舶保安評価と港湾施設保安評価がある。ここで「港湾施設」とは、「港湾のうち船舶とのインターフェイスとなる部分」を意味し、錨地等を含む。この言葉は、SOLAS 条約の適用範囲を考慮して定義されたものである。

4　保安評価の手順

4.1　保安評価の概略の手順

保安評価の概略の手順を図 3 に示す。

「脅威の同定（threat identification）」は安全評価における「ハザード（hazard）の同定」に相当する。次に、安全評価において事故シナリオが作成されるのと同様に、同定された脅威に対してシナリオが作成される。なお、評価に要する作業の軽減のため、脅威の優先度が検討され、重要な脅威についてのみシナリオが作成される場合もある。保安評価のシナリオは、一般に、Event Tree Analysis 等により詳細に解析されることはなく、その数が膨大になることは無いため、シナリオのグループ化は行われない。安全評価における事故シナリオの発生確率の評価及び損害の期待値の評価に相当するのが、シナリオの蓋然性の評価及び結果の評価である。シナリオの結果は、被害の規模として表現されるのが一般的であるため、以下「被害規模」と呼ぶ。一般に保安評価は、定量的なものではない。また、蓋然性評価においては、主観の排除すら十分になされているとは言い難い。蓋然性と被害規模の積が各シナリオに起因するリスクとなる。安全評価では、全ての事故シナリオに起因するリスクの総和が、解析の対象が保有するリスクとなる。しかし保安評価では、各シナリオによるリスクの総和を評価するよりも、個々のシナリオが許容できるか否か、または、蓋然性或いは被害規模の有効な低減策があるか否かが検討される場合が多い。この点については後述する。なお、船舶の保安評価では、ISPS Code により現場保安検査（On-scene security survey）が要求されている。ISPS Code は、保安対策を定期的に見直すことを要求しており、保安評価は定期的にやり直す必要がある。この点について次に述べる。

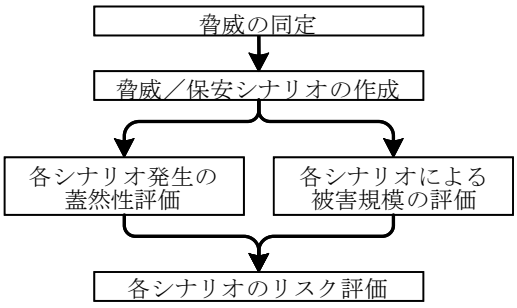

図 3　保安評価の手順

4.2　最新情報の入手

有効な保安対策はその時々で変化する。そのため、保安評価も定期的にやり直す必要があり、保安評価においては最新情報の収集が、安全評価の場合以上に重要と考えられる。以下では、代表的脅威の一つとして、海賊を例にとって最新情報の重要性を示す。なお、「海賊（Piracy）」は国連海洋法条約により公海上における暴力行為等と定義されており [6]、領海内における行為は IMO 等において「船舶に対する武装強盗（armed robbery against ships）」と呼ばれている。ここではこれらを総称して「海賊行為」と呼ぶ。

図 4 は、地域別の海賊行為の発生件数である [7]。図より、近年マラッカ・シンガポール海峡等、東南アジアの海賊行為が減少している一方、アフリカにおいて海賊行為が増えていることが分かる。

図 5 は、海賊行為による被害者の数の推移を種類別に示したものである。図より、2008 年になって、捕虜・誘拐等、人質に取られる乗組員（一部、乗客を含む。）の数が増えていることが分かる。2008 年における誘拐等の海賊行為の多くは、ソマリア沖・アデン湾で発生している。この海域はインド洋とスエズ運河を結ぶ水路にあたるため、海賊による脅威が高まったことにより、スエズ運河を避けて喜望峰回りの航路を選択する船が 250 隻以上に達したとの報道もある [8]。こうした海賊行為の防止のため、国際連合安全保障理事会の決議に基づき [9]、本稿執筆時点（2009 年 1 月）において、複数の国がこの海域に軍を派遣している。また、国内においても、海上自衛隊の艦艇のソマリア沖への派遣について検討されている。

海賊行為の例からも海事の保安に関する脅威は時々刻々変化することが分かり、保安評価においては最新情報の収集が重要であると言える。

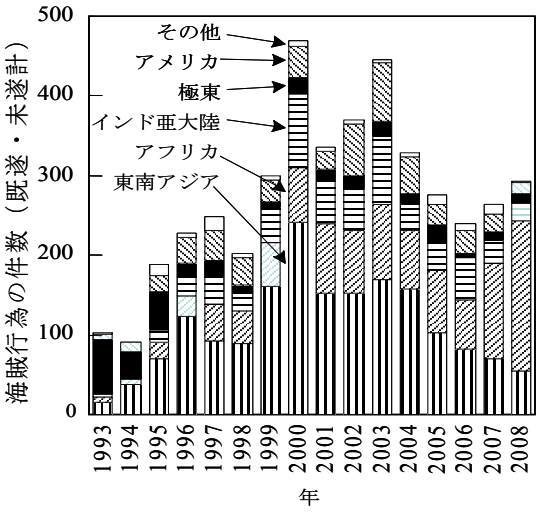

図 4　地域別海賊行為件数の推移

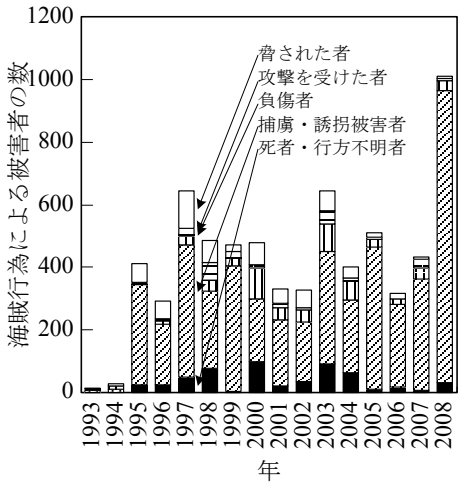

図 5　被害の種類毎の人数の推移

4.3　脅威の同定

船舶の保安評価を例にとると、脅威の同定において考慮すべき事項としては以下が挙げられている（c.f. ISPS Code, Part B, 8.9 節）。

.1　船舶の破壊（爆破、放火等）
.2　船舶のハイジャック／拿捕
.3　貨物の不正開梱／重要な船舶装置・設備の不正改変
.4　不正侵入（密航を含む）／不正使用
.5　大量破壊兵器等の武器等の密輸
.6　テロリスト等の乗船／船舶の利用
.7　武器／破壊の道具としての船舶の利用
.8　停泊／錨泊中の海上からの攻撃
.9　海上における攻撃

港湾施設については、ISPS Code の他に ISO 規格 [10] にも記述があるが、ここでは詳細には言及しない。

4.4　シナリオの作成及び蓋然性の評価

例えばテロによる破壊活動という脅威に関するシナリオを作成するには、船舶の活動範囲や船種・船型、必要に応じて国籍等も考慮して、行為者（テロリスト）及び代表的な手口を想定した上で、如何なる破壊活動がなされる可能性があるかを記述していく。シナリオを作成する際には、テロ等に関する最新の情報を考慮する必要がある。

シナリオの蓋然性の定量的評価 [11) to 13)] は、現時点では容易ではなく、保安評価において最も恣意性が入りやすいのはシナリオの蓋然性評価だと考えられる。そのため ILO と IMO が作成した港湾の保安に係る基準 [14] では、蓋然性に代えて脆弱性、即ち攻撃成功の容易さやテロ等に対する防御の弱さを用いる方法を示している。しかしながら、定性的ではあっても「リスク」を求めるからには、

蓋然性、即ち攻撃成功確率に相当する値を、脆弱性、即ち攻撃実施の容易さで置き換えることは、正否を別とした攻撃そのものの発生確率を無視することになり、適当ではない。このことは、船舶の衝突確率を評価するのに「避航操船失敗確率のみを考慮し、避航操船が必要な状況の発生確率を無視する」のが不適当であることから、容易に理解できるであろう。それでもなお、国際基準[14]においてこうした置き換えが行われた理由、即ち必ずしも合理的ではないリスクの検討が推奨されている理由は、「攻撃が発生する確率」の評価が困難であることに加え、「攻撃発生確率が低い」との恣意的な判断により保安対策を実施しない港湾が増えることを避けるためと考えられる。

4.5 シナリオによる被害規模の評価

シナリオによる被害規模の評価は、科学的知見に基づいて行われる場合もある。危険物ばら積み船が攻撃を受けるというシナリオに関する被害規模を評価する際の手順の例[15) to 18)]を図6に示す。

簡単に説明すると、想定されたシナリオに基づき、構造損傷、貨物である危険物（引火性液体または液化された可燃性気体）の流出、海面上の拡散の順に評価し、直ちに着火した場合の海面火災（プール火災）と、着火せずに蒸発した場合の可燃性ガス（蒸気）の移流拡散（蒸気雲拡散）を推定し、さらには蒸気雲に着火した場合の熱や圧力変動を評価し、その上で、別途設定する熱や圧力のクライテリアを考慮して、影響範囲を決めるという手順になる。さらに、停泊中の船舶への攻撃を想定した場合、影響範囲の人口や事業所の従業員数[19)]が調べられる場合もある。

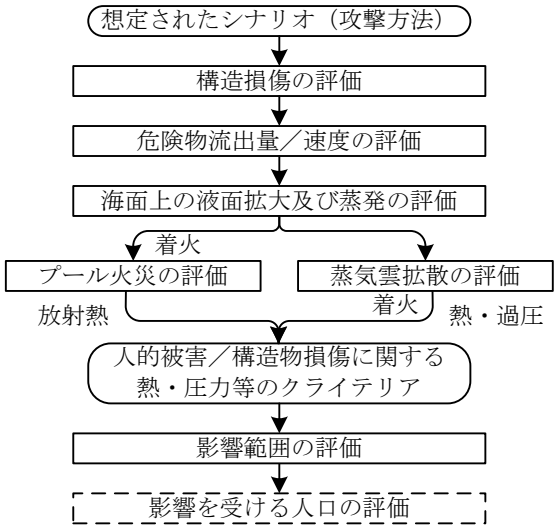

図6 被害規模評価手順の例
（引火性液体等ばら積み運搬船等の場合）

シナリオに基づく影響範囲等の推定結果は、リスク解析の目的のみならず、避難計画策定の基礎としても用いられる。大規模なテロ等の事態が発生した場合の避難計画は、都道府県知事により作成されるが[20), 21)]、テロ攻撃の影響範囲の推定は、そうした計画の検討の基礎となる。そのため、影響範囲の推定は、保安に係るリスクの評価とは別に実施される場合がある。

4.6 リスクに基づく判断

安全評価であれば、各シナリオの発生確率と損害の期待値の積の総和、即ちリスクを求め、そのリスクに応じて、さらなる安全対策の要否を判断するといった方法がとられる。しかし、保安評価では、リスクを定量化しないまま、蓋然性が高く、且つ、被害規模が大きいシナリオがあれば、そうしたシナリオを排除するための保安対策を取るべきと判断するのが一般的である。蓋然性も被害規模も、いわゆるランキングで表現される場合が多いため、例えば表1のような判断基準が推奨されている例[10)]がある。

5 保安対策

保安評価の主な目的は保安対策の決定である。そのため保安評価は、安全評価の場合と同様に、各種対策の効果を評価できるものでなくてはならない。しかしながら前述の通り、保安評価は、ある種の被害規模推定を除けば、科学的根拠に基づく定量的評価とは言い難く、各種対策の効果の評価も定性的である。実際には、保安対策の有無や実施の水準に関するチェックリストを用意しておき、そのチェックリストを勘案して脆弱性や蓋然性を大雑把に評価する場合が多い。

保安対策の主たるものは、アクセスの制御（Access Control）であり、具体例としては、以下が挙げられる。

- 塀の設置／出入り口の管理（港湾）
- 立ち入り禁止区域／立ち入り権限の設定
- 保安要員の配置／周辺の監視
- 関係者・来訪者の登録／認証
- 来訪者への関係者による付き添い
- 資料の閲覧／利用の権限の設定
- 危険な海域の回避／航行時刻の選択（船舶）

表1 追加保安対策の要否判定方法の例

		被害規模		
		大	中	小
蓋然性	高	対策追加	対策追加	―
	中	対策追加	―	―
	低	―	―	―

アクセスの制御では、身元等が不明確な人間を、然るべき場所に立ち入らせないことが肝要である。そのため米国では、特定の港湾に出入りするトラック運転手等に TWIC カード [22]と呼ばれる身分証明書の携帯を義務づけている。また、出港前の密航者に対する点検も重要である。参考のため、密航事件及び密航者数の推移 [23]を図 7 に示す。図より、近年密航が増加していることが分かる。

アクセスの制御のためには、挙動不審者の識別も必要であり、IMO が刊行する保安要員の訓練モデルコース [24]には、そのための指針がある。参考のため指針の内容を付録に示す。

各種シナリオの蓋然性を低減する対策の代表的なものはアクセスの制御であるが、被害規模を低減する対策は、船舶について言えば、事故後の対策と概ね同様であり、消火、避難、退船等の対策が有効と考えられる。但し、通常の事故後と対応が異なるのは、テロによる爆発物の使用が疑われる場合である。こうした場合、むやみに現場に近づいてはならない [25]。これは、爆発物は複数仕掛けられている可能性が高いためである。よって、通常の火災であれば発生後は速やかに消火にあたるべきであるが、爆弾テロが疑われる場合はその限りではない。

6　おわりに

船舶や港湾においても保安対策は必要であり、船会社や港湾管理者は一定程度の対策を実施すべきと考えられている。一方保安対策には、制度面の対策や軍事に相当するものもあり、個々の事業者だけが実施すべきものではない。そのため、保安対策の評価は、各種政策の評価をも含むと考えられ、テロ対策については国家保安（National Security）といったレベルで論じられることもある。ここでは、ISPS Code で要求される保安評価を中心に、船舶や港湾におけるリスクや対策について述べたが、これは、政策評価を論じるに充分な知見を著者が有しないことによる。セキュリティーの研究は我が国では黎明期にあり、保安評価も引き続き研究すべき課題だと考えられる。

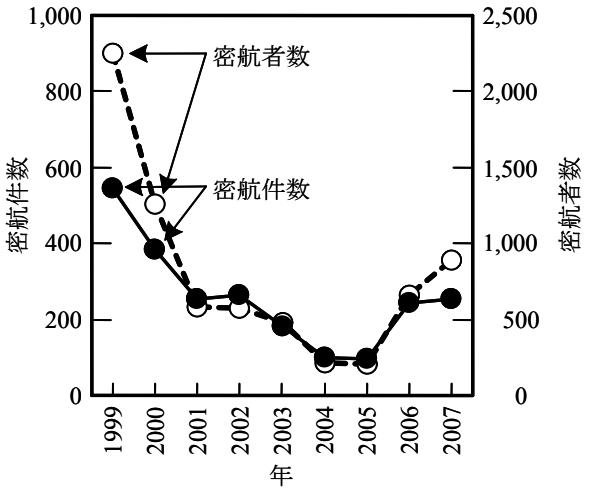

図 7　密航事件・密航者数の推移

参考文献

1) Lloyd's Register Fairplay (LRF) casualty data, 1978 to 2007
2) "Vulnerability Assessment of Physical Protection Systems", Mary Lynn Garcia, Sandia National Laboratories, 2006
3) SOLAS Convention, Annex Chapter XI-2 "Special measures to enhance maritime security"
4) "International Code for the Security of Ships and of Port Facilities"
5) 「国際航海船舶及び国際港湾施設の保安の確保等に関する法律」及び「同施行規則」
6) United Nations Convention on the Law of the Sea, 1982, Article 101
7) ICC International Maritime Bureau Piracy and Armed Robbery against Ships - Annual Report, 2003 年版、2005 年版、2006 年版、2007 年版及び 2008 年版
8) TradeWinds, 2009 年 1 月 16 日付記事 "Suez suffers", by Gary Dixon http://www.tradewinds.no/
9) 国連安全保障理事会決議
第 1816 号：2008 年 6 月 2 日及び
第 1838 号：2008 年 10 月 7 日
第 1846 号：2008 年 12 月 2 日
10) ISO 20858:2007 "Ships and marine technology -- Maritime port facility security assessments and security plan development"
11) USCG: NVIC (Navigation and Vessel Inspection Circular) 10-02: Security Guidelines for Vessels, 2002
12) USCG: NVIC (Navigation and Vessel Inspection Circular) 11-02: Recommended Security Guidelines for Facilities, 2002
13) Norwegian Shipowners' Association: Guideline for performing Ship Security Assessment, 2003
14) ILO/IMO Code of practice on security in ports, 2003

15) Mike Hightower, et al., "Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill Over Water", Sandia National Laboratories, 2004
16) ABSG Consulting Inc., "Consequence Assessment Methods for Incidents Involving Releases from Liquefied Natural Gas Carriers", 2004
17) Anay Luketa, et al, "Breach and Safety Analysis of Spills over Water from Large Liquefied Natural Gas Carriers", Sandia National Laboratories, 2008
18) H. Oka & S. Ota, "Evaluation of Consequence Assessment Methods for Pool Fires on Water Involving Large Spills from Liquefied Natural Gas Carriers", Journal of Marine Science and Technology Vol.13, No.2, 2008
19) 統計データ・ポータルサイト（政府統計の総合窓口）http://www.e-stat.go.jp/（2008 年 4 月より運用開始。2008 年 11 月時点）
20) 武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律
21) 武力攻撃事態等における国民の保護のための措置に関する法律
22) Transportation Security Administration - WEB SITE: http://www.tsa.gov/
23) IMO FAL.2/Circular No. 63, 71, 77, 83, 89, 95 & 102
24) IMO, Model Course 3.19: "Ship Security Officer", Model Course 3.20: "Company Security Officer", & Model Course 3.21: "Port Facility Security Officer", 2003
25) ハイム・グラノット、ジェイ・レビンソン、「イスラエル式テロ対処マニュアル－爆弾テロ対応の手順」、2004

付録 IMO モデルコースの指針
「差別的でない判断に基づく潜在的な保安上のリスクを引き起こす人物の認知」

（例えば、Model Course 3.20: "Company Security Officer"第 7.4 節）

指導員は、人種による分析や民族的な偏見を避けることの重要性を強調しつつ、疑わしい行動パターンを解説することが求められる。疑わしい行動パターンの例を以下に示す。

- 船舶または施設を撮影する身元不明の人物
- 船舶または施設に立ち入ろうとする身元不明の人物
- 施設に隣接してまたは施設の近隣で、商売や屋台を営む人物
- 長期間にわたり船舶または港湾施設に近接する地域を徘徊する身元不明の人物
- 保安、従業員、または通常の業務手順について施設に電話で問い合わせる身元不明の人物
- 付近を徘徊し船舶または施設を撮影するまたは見取り図を作成することが疑われる人物を乗せた車両
- 付近を徘徊し船舶または施設を撮影するまたは見取り図を作成することが疑われる人物を乗せた小型船舶
- 船舶または施設の近隣上空を飛行する一般航空機
- 爆弾を所持するまたは自爆行為に関与する可能性のある人物
- 従業員またはその家族に接近し会話を交わし船舶または施設に関する情報を入手しようと試みる身元不明の人物
- 商品を売ろうと試みる行商人
- 機器の修理、交換、点検、または設置のために施設に入ろうとする作業員
- 施設、従業員、または通常の業務手順に関する情報を入手しようと試みる電子メール
- 配達されたおよび配達を試みられた小包
- 従業員または行商人が表す反国家的感情
- 従業員に配布されたまたは駐車場で車両のフロントガラスに置かれた反国家的パンフレットやビラ
- 通常でない電話
- 他の船舶からの支援を求めようと遭難中の船員を装うレジャー用船舶または難民船上の人物