

国土技術政策総合研究所資料

TECHNICAL NOTE of
National Institute for Land and Infrastructure Management

No.585

March 2010

海上輸送を中心とした最近のサプライチェーン セキュリティの動向（その2）

岩瀬美奈子・和田匡央・箕作幸治・安部智久

Recent Development of Supply Chain Security
Related to Maritime Transport(Vol.2)

Minako IWASE,Masao WADA,Koji MITSUKURI,Motohisa ABE

国土交通省 国土技術政策総合研究所

National Institute for Land and Infrastructure Management
Ministry of Land, Infrastructure,Transport and Tourism,Japan

海上輸送を中心とした最近のサプライチェーン セキュリティの動向（その2）

岩瀬美奈子*・和田匡央**・箕作幸治***・安部智久****

要 旨

企業がサプライチェーンを世界規模で構築・運営して効率化を図る一方、先の米国同時多発テロを契機に国際輸送分野での保安対策の強化に向けた動きが進展している。港湾・海事分野における SOLAS 条約での ISPS コードによる保安対策に加え、サプライチェーン全体についての保安対策も進みつつあり、これは港湾保安の分野においても様々な影響を及ぼす可能性がある。

本資料では、現在実施ないしは検討が進められているサプライチェーンにおける海上輸送保安対策の世界的動向について整理し、かつそれが今後の港湾に及ぼしうる影響について考察を行うものである。

キーワード： サプライチェーンセキュリティ、AEO、貨物追跡システム、100%スキャンニング

* 管理調整部 国際業務研究室 研究官
** 管理調整部 国際業務研究室 室長
*** 管理調整部 主任研究官
****財団法人 国際臨海開発研究センター
〒239-0826 横須賀市長瀬3-1-1 国土交通省国土技術政策総合研究所
電話：046-834-9584 Fax：046-834-9843 e-mail: iwase-m83ab@ysk.nilim.go.jp

Recent Development of Supply Chain Security Related to Maritime Transport(Vol.2)

Minako IWASE*
Masao WADA **
Koji MITSUKURI **
Motohisa ABE***

Synopsis

While firms tend to develop supply chain on global scale, various initiatives to secure international logistics network has been proposed or implemented, after the 9/11 incident.

The initiatives cover not only port/maritime sector in which security measures are already in action under SOLAS/ISPS Code, but also total supply chain. And there is a possibility that the measures will affect various activities in ports, as well as countermeasures for port security.

In this note, the recent developments of such security initiatives are to be reviewed, and a few examinations are to be given as to the influence by the initiatives on ports.

Key Words: Supply Chain Security, AEO, MATTS, 100%Scanning

* International Affairs Study Division, NILIM
3-1-1 Nagase, Yokosuka, 239-0826 Japan

Phone : +81-468-34-9584 Fax : +81-468-34-9843 e-mail: iwase-m83ab@ysk.nilim.go.jp

** Dept. of Administration and Coordination, NILIM

***The Overseas Coastal Area Development Institute of Japan

目 次

1. はじめに	1
2. サプライチェーンセキュリティの動向	1
2.1 AEO 制度の現状および相互認証への取組状況	1
2.2 10+2 ルールの現状	2
2.3 Non-SOLAS 船対策の現状	2
2.4 その他の取組	3
3. 港湾における国際輸送セキュリティ導入のための検討	3
3.1 RFID 導入のための検討	3
3.2 100%スキャニング法導入のための検討	5
4. その他のセキュリティ対策の検討	7
4.1 トレードリカバリープログラムの検討	7
4.2 セキュリティコストの現状	7
5. 考察	8
6. おわりに	8
参考文献	9
謝辞	9
参考:英用語の略号	10

1. はじめに¹⁾

2001年9月11日の米国同時多発テロ事件発生から早くも8年が経とうとしている。

この8年間に、主要国・国際機関において国際輸送に関するセキュリティ対策が進展してきていることについては、国総研資料 No.528 で述べた。

この8年間に、物流のセキュリティ対策は、港湾での水際対策からサプライチェーン全体での安全を確保する対策へと進展し、現在までにさまざまな対策が取られてきた。

なお、サプライチェーンセキュリティを確保する方法としては下記の5項目¹⁾、

- ① コンテナの内容物の物理的検査（スキャンニング）
- ② コンテナの保全性（シール技術）の確保
- ③ コンテナ輸送環境の保全
- ④ コンテナの追跡
- ⑤ 貿易文書及び輸出入貨物情報の管理

があり、港湾への影響が大きいと考えられることは国総研資料 No.528 で述べた。

そこで、本資料では、第二章においてセキュリティ対策の最新の動向を引き続き収集した結果を述べる。更に、第三章では日本の港湾へ対策を導入するにあたり、港湾へ影響を与える問題点を整理した結果を述べ、第四章ではこの5項目以外の新たな対策の必要性について述べる。

2. サプライチェーンセキュリティの動向

現在取り組まれているサプライチェーンセキュリティの対策で、重点的に強化されている対策は、第一章で述べた⑤貿易文書および輸出入貨物情報の管理である。よって、ここでは、貿易文書および輸出入貨物情報の管理にあたる、AEO*制度(Authorized Economic Operator：認可事業者制度)と10+2ルール(importer Security Filing Additional Carrier Requirements：輸入者セキュリティファイリングルール)について述べる。また、その他に強化されつつある対策である、Non-SOLAS 船対策などについての現状について述べる。

2.1 AEO 制度の現状および相互認証への取組状況²⁾

AEO 制度とは、民間企業と税関のパートナーシップを通じて、国際物流におけるセキュリティ確保と物流効率化を両立させる制度であり、現在は、米国の C-TPAT (Customs Trade Partnership Against Terrorism：テロ行為防

* 英用語の略語は巻末に添付する。

止のための税関・産業界パートナーシップ)を始めとして、各国において制度が設けられている。そこで、ここでは、日本の AEO 制度の紹介と、各国との相互認証の状況について述べる。

1) 日本における AEO 制度の現状

日本における AEO 制度は、下記のとおり6つの制度がある。

- ① 特例輸入申告制度 (対象業種：輸入者)
- ② 特定輸出申告制度 (対象業種：輸出者)
- ③ 特定保税承認制度 (対象業種：保税蔵置場等の被許可者)
- ④ 認定通関業者制度 (対象業種：通関業者、船会社、航空会社、貨物利用運送事業者 等)
- ⑤ 特定保税運送制度 (対象業種：国際運送業者、倉庫業者、CY 管理者、認定通関業者)
- ⑥ 認定製造者制度 (対象業種：製造者)

業種によって取得対象となる制度やメリットが異なるが、いずれの制度においても認定されるには、コンプライアンスに優れていることが必要となる。また、貨物の安全管理体制についても優れていることが必要である。貨物の安全管理の一例を表-1 に示す。

表-1 貨物の安全管理の一例

貨物管理の例
<ul style="list-style-type: none"> ・ 貨物管理施設の障壁、壁、扉、施錠機構等に損傷はないか。 ・ 貨物管理施設の監視カメラは正常に作動するか。 ・ 貨物管理施設は警備員による巡回等は行われているか。 ・ 貨物管理施設外部からの不正なアクセスを防止するための設備等に異常はないか。 ・ 貨物の搬出入の際のチェックは厳正に行われているか。 ・ 出入りする従業員、外来者及び車両のチェックは厳正に行われているか。 ・ 過剰輸送コンテナの壁内等のチェック、コンテナへの施封等は適正に行われているか。 ・ 空の海上輸送コンテナは適正に保管管理されているか。 ・ 在庫貨物の保管・出庫管理は適正に行われているか。 ・ 移動中の貨物について、その所在地等の把握は的確に行える体制が維持されているか。 ・ 不審者が侵入等した場合には、適切に対処できる体制が維持されているか。 ・ 不審貨物又は異常のある貨物等があった場合には、適切に対処できる体制が維持されているか。

なお、AEO 制度の大きなメリットとして、通関時間の短縮が挙げられる。AEO 制度を利用した場合の貨物の輸入通関時間は、わずか0.1時間であり、通常海上貨物の通関時間の3.1時間と比べて大幅に短くなっていることが税関の調査²⁾によりわかっている。

2) 我が国の相互認証への取組状況²⁾

米国の C-TPAT と日本の AEO 制度の相互認証が 2009 年 6 月 26 日に合意に達した。

相互認証の取り決めは、日本ではニュージーランドに続く 2 例目で、米国では、ニュージーランド、カナダ、ヨルダンに続く 4 例目である。

米国との相互認証の取り決め内容は以下の 4 点である。

- (1) 米国税関当局は、輸入貨物の審査・検査の際、当該貨物が我が国の AEO 企業による輸出貨物である場合には、その資格をリスク評価に反映させる。
- (2) 両国税関当局は、自国の AEO 制度に関して相手国企業を審査する場合に、当該企業が相手国の AEO 企業であるときは、その資格を受け入れる。
- (3) 両国税関当局は、有事の際に AEO 企業の貨物を優先的に取り扱う共同の仕組みの構築に向け努力する。
- (4) 両国税関当局は、一般に各種のセキュリティ関連措置の適用に当たり、相手国の AEO 企業に対しては、権限の範囲内かつ可能な限りでその資格を考慮に入れるべきである。

現在日本では、EU やカナダとの相互認証に向けた取組を行っている。

また、日本機械輸出組合へのヒアリングによれば、「C-TPAT は輸入貨物のみが対象であるため、日本からの輸出貨物に限定されるが、将来的には、相互認証が進み米国の C-TPAT 認証企業と我が国の AEO 認証企業間であれば相互で日本からの輸出貨物の通関手続きと米国への輸入手続きを同時に実施できることが理想である。」とのことであった。

2.2 10+2 ルールの現状³⁾

10+2 ルールは、2009 年 1 月 26 日から暫定的に施行されている貨物の事前申告制度であり、2010 年 1 月 26 日から本格導入が行われている。

10+2 ルールとは、米国の輸入者（または代理人）が、米国向けに船積みする 24 時間前までに、要求されている 10 項目を、船社については要求されている 2 項目を CBP(U.S. Customs and Border Protection : 米国税関・国境警備局)へ電子申請する規則である。申告の後、申告した情報に不備等があった場合は“Do not load”（船積み不許可）となる。しかしながら、この“Do not load”のメッセージは、申告した米国の輸入者（または代理人）ではなく、船社に送信されるため、輸入者と船社との連絡を密にする必要がある。

10+2 ルールの実施にあたっては、各企業とも 10+2 ルール

で提出しなければならない内容について、時間内に申告できるシステムにはなっていないため、サプライチェーン全体を通してシステムの再構築を行うことが必要となった。更に、この 10+2 ルールの申告の手数料として、1 申告あたり 10~50 ドルかかるとの報告もある。以前、24 時間ルール実施時にもシステムの変更が必要となり、船社から荷主へ、1 船荷証券当たり 25~30 ドルの手数料が発生している⁴⁾。

なお、米国内に拠点のある業界団体からは「10+2 ルール」に対する要望として、下記の点が挙げられている。

- ① C-TPAT 認定企業に対して優遇措置を与えること
- ② 「10+2 ルール」で収集される機密企業情報が外国政府など第三者に開示されないことを CBP が保証すること
- ③ CBP が「10+2 ルール」の導入が確実に国家セキュリティを改善することを実証すること
- ④ 輸入者が各企業の積荷の状態を明らかに把握できるように、CBP が輸入者に対して輸入者セキュリティ・ファイリング受領確認メッセージを提供すること⁵⁾

2.3 Non-SOLAS 船対策の現状⁶⁾

IMO(International Maritime Organization : 国際海事機関)では、2002 年 12 月に改正 SOLAS 条約が採択された後も、確実な海事保安対策が実施されるための具体的な方策が検討されている。この中で、Non-SOLAS 船の保安ガイドラインについても審議されている。

2008 年 11 月に開催された第 85 回 IMO 海上安全委員会(MSC85)では、Non-SOLAS 船の保安強化のためのガイドラインが承認された。

このガイドラインは、改正 SOLAS 条約の効力の及ばない、「旅客を伴わない商船」「旅客船」「漁船」「プレジャーボート」に対して、リスク評価に基づき、リスクに見合った適切な対策を実施することを促すものである。ただし、これはあくまでもガイドラインとしての取り扱いであり、強制ではない。

このガイドラインの内容は、「リスク評価」「保安の認識と文化」「保安対策」「保安事案に対する計画」「国際航海のためのその他の保安考慮事項」から成っており、リスク評価を行うことの重要性、保安宣言や従業員管理の必要性、盗難やハイジャック防止のためのグッドプラクティス、緊急時対応計画とその訓練・操練の実施の必要性について記載されている。詳細は表-2 のとおりである。

表-2 Non-SOLAS 船の保安ガイドライン

項	目	内	容
1	リスク評価	<ul style="list-style-type: none"> ・ リスク評価を行うことの重要性 ・ リスク評価のための参考資料、ツールの紹介 	
2	保安の認識と文化	<ul style="list-style-type: none"> ・ 保安宣言(DoS)について ・ 保安レベルの概念について ・ 訓練や従業員管理の必要性について ・ Non-SOLAS 船に保安宣言(DoS)を要求する際に必要な手続きについて(改正SOLAS条約適合港湾および船舶の保安管理者向け) 	
3	保安対策	<ul style="list-style-type: none"> ・ 小型船やプレジャーボートがテロリストによる攻撃に使用された事例 ・ 保安対策のグッドプラクティスについて ex. 船の盗難、ハイジャック防止対策 船への不正アクセスの防止策 船内捜索の実施 乗船者の身元確認 利用可能な船舶識別手段の活用 サプライチェーンセキュリティ国際基準(ISO28000シリーズ) 	
4	保安事案に対する計画	<ul style="list-style-type: none"> ・ 緊急時対応計画 ・ 訓練や操練の実施の必要性 ・ 爆発物が仕掛けられたおそれのある場合等の対応 ・ 保安にかかわる関係当局等への報告の必要性 	
5	国際航海のためのその他の保安考慮事項	<ul style="list-style-type: none"> ・ 国際航路の就航するNon-SOLAS船が留意すべき事項 ・ 海賊行為からの回避、麻薬取引・不法貨物輸送の防止、密航者の防止について 	

一方、米国水域には、登録されたプレジャーボートが約 1,300 万隻活動しており、これらの小型船舶を使った 2000 年 10 月に起こった米海軍ミサイル駆逐艦コール号事件のような自爆テロ等への大きな懸念がある。また、2008 年 11 月に発生したインドのムンバイでの同時多発テロにおいて、テロリストがボートにて港から上陸したこともあり、米国において小型船対策についての関心が高まっている。

シンガポールにおいては既に独自に小型船への AIS(Automatic Identification System：自動船舶識別装置)の搭載を行っており、いち早く Non-SOLAS 船対策に取り組んでいる。AIS 装置の搭載のメリットは、

- ・ 安全と保安の強化
- ・ 海難事故や負傷者発生の際の対応の迅速化
- ・ 窃盗や不正取引防止強化
- ・ 不法な漁業行為防止強化 等 IMO によると

が挙げられている。

以上のように、改正 SOLAS 条約の対象にならない小型船舶についての対策を行っている国もある。

2.4 その他の取組⁷⁾

ISPS コード(International Ship and Port facility Security Code：国際船舶および港湾施設の保安コード)では海中のセキュリティまでは規程されていないが、現在では、海中での港湾セキュリティ強化の対策のための機器も開発されている。それが、海中ソナーである。

海中ソナーには、QinetiQ 社製のケルベロス・スイマー探知ソナーや、Lockheed Martin Canada 社製のスイマー探知ソナー(SDS)、C-Tech 社製の CSDS-85 オムニ・アクティブ監視ソナーなどがある。

ケルベロス・スイマー探知ソナーは、深度 800m までの範囲で脅威を探知することができ、船体に装備し、船舶下方の 360° の範囲の探査や、海底に敷設し、岸辺や沖合施設を 360° 監視することができる。

SDS は、港湾や核施設、製油所やパイプラインなどの防護及び、海上の船舶を海中の侵入者から守る目的で設計されている。

CSDS-85 オムニ・アクティブ監視ソナーは既に使用されており、港湾監視、発電所やパイプラインなど沿岸施設の周辺監視、沖合の石油掘削装置や船舶の防護に使用されている。CSDS-85 も海底や棧橋、船舶に装備することが可能で、海中から制限区域への侵入者を探知するように設計されている

これらの機器については、今後、海中からの侵入者によるテロが発生した場合、注目されることが予測される。

3. 港湾における国際輸送セキュリティ導入のための検討

本章では、港湾の整備・運営を行うにあたり影響を与えることが懸念される、「RFIDを活用した貨物追跡システム」と「100%スキャン」について、今後導入する場合に問題となる事項について検討を行った。

3.1 RFID を活用した貨物追跡システム導入のための検討⁸⁾⁹⁾

国総研資料 No.528 で述べたように、サプライチェーンセキュリティを確保する方法の一つとして、コンテナの保全性(シール技術)の確保が挙げられる。

現在までのところ、シール技術の一つとして、RFID(Radio Frequency Identification：電波による非接触型自動認識技術)の開発が進められており、ISO においては国際標準化が進められ、EPCglobal においては国際標準規格化

への働きかけが行われている。

RFIDは、物流管理の分野では既に利用されており、更にRFIDを保安対策へ活用することが検討されている。このRFIDの保安対策への活用の取組が、物流可視化、すなわち貨物追跡システムへの取組である。これらの貨物追跡システムの実用化に向けて、DHS、EPCglobalなどが、貨物追跡システムの実証実験を行っている。

このように、RFIDを活用した貨物追跡システムは、今後世界的に導入されることが予測される。よって、本章では、日本の港湾において導入するための課題の抽出を行う。

1) MATTSの取組

MATTS(Marine Asset Tag Tracking System: 海上貨物追跡タグシステム)とはDHSにて開発が進められている海上貨物追跡タグシステムのことで、日本においては国土交通省港湾局が支援し、実験を行っている。

MATTSの目的は、コンテナ貨物のセキュリティ確保であり、海上コンテナの位置情報やドアの開閉などを含めたセキュリティ情報をリアルタイムでモニターできる可視化システムを目指している。2006年から実験を開始し、2007年4月～8月と、2008年7月～2009年6月に実証実験が行われた。

まず、第一回目の実証実験では、データ転送の確実性・速度などの通信機能、GPSによる測位機能、電力供給性能・取付具合などの実用性などの検討が行われ、第二回目の実験ではサプライチェーンへの適用の検討が行われた。

その結果、成功を収めたため、今後は世界規模での普及に向けていく予定とのことである¹⁰⁾。

このMATTSに必要なシステムは、表-3の通りであり、港湾においては、iTAGやmLOOKなどのRFIDタグの情報を吸い上げる受信機である、iGATEの設置が必要となる。また、iTAGやmLOOKの位置情報を画像にて管理するために、iVIEWサーバーが必要となる。

表-3 MATTSに必要な機器

機器名	役割
iTag	GPS測定機能、モーションセンサー、ログ、自動記録、ZigBee通信、携帯通信性を確保したデバイス。位置情報取得を行う
mLock	iTagの機能に加えてコンテナの開封を監視する電子シール機能を備える
iGATE	ZigBee(低消費電力)通信機能、インターネットゲートウェイ機能、GPS測位機能を有するアンテナ。iTagの情報を吸い上げる。
iView	iTagデータ表示、タグー表示、データ経歴表示、アラーム情報表示、タグへの遠隔指令機能を有するソフト。これにより管理を行う。

2) EPCglobalの取組

EPCglobalとは、流通業界を中心としたバーコードの国際標準化を推進するGS1の下部組織で、RFIDの国際標準化を推進する非営利法人である。

EPCglobalには4つのグループが活動しているが、そのうちの国際物流部会(Transportation & Logistics Services)にて、荷主企業-物流企業間での貨物の可視化についての海上輸送・航空輸送における実証実験が行われている¹¹⁾。

EPCglobalでの実証実験の目的は、業務の効率化および省力化の実現と国際貿易のセキュリティ確保であり、企業が自社製品のサプライチェーン全体を追跡できるシステムを目指している。

実証実験は、2007年1月～2月、12月、2008年12月～2009年2月の3回行われた。

まず、2007年1月～2月の第1回目の実証実験において、読み取られた情報がリアルタイムでフォワーダー、荷主、ターミナルオペレーターなど全関係者で共有できるかについての実証を行い、同年12月の第2回目の実証実験にて、荷主・物流会社間の情報共有基盤の検証を行った。更に、2008年12月～2009年2月までの第3回目の実証実験では、国際物流において貨物輸送状況の自動認識および、発地から着地までの貨物輸送情報を関係者間で共有できるかについての検証を行った。

その結果、海上輸送の環境下において、荷姿に応じた種々のRFIDタグから取得した輸送情報と商品取引情報を紐付けることにより、サプライチェーン場のすべての関係者間で貨物輸送情報を共有できることが実証できた。現在、この実験結果を国際標準規格団体であるEPCglobalの標準規格審議にフィードバックしている。

3) SECCONDDプロジェクトの取組¹²⁾

一方、EUにおいても、SECCONDD(Secure Container Data Device Standardization: 安全コンテナデータ装置)プロジェクトと呼ばれる、移動中のコンテナのモニタリングに関する世界標準を策定中である。

SECCONDDプロジェクトの目的は、スマートコンテナあるいは車両に記録された情報を、港や国境通過時に法執行当局者や貿易担当当局者が読み取れるよう、国際標準を創出することである。また、このSECCONDDプロジェクトでは、内蔵のセンサーから、保管情報、コンテナの経由地、爆発装置や人などが途中で入った形跡の有無、有害物の有無を把握することができるシステムを目指している。

4) まとめ

1)～3)の取組の他にも、港湾ターミナル運営会社である Hutchison Port Holdings 社が Savi Technology 社と RFID ネットワークを世界規模で構築することを目指すと発表している。このように、世界の情勢は RFID を利用した物流管理の方向へ進化している。しかしながら、これは Hutchison Port Holdings 社などの港湾ターミナルを運営している港間での物流に限られ、世界的なサプライチェーンセキュリティにはつながっていない。

このように、RFID の保安対策への活用が普及しない背景として、

①サプライチェーン全体での責任の所在とシステムの管理主体が不明確。

②コスト面から、保安対策のみを目的とした導入は困難。との理由が挙げられる。

①の、責任の所在とシステムの管理主体に関する問題については、MATTS、EPCglobal、SECCONDD において共通する事項であり、サプライチェーンは1国内のみでなく、数カ国にまたがっているため、システムの管理を誰がどのように行うのかを決めることが難しいと考えられる。例えば、A 国と B 国間の通信回線に不具合が生じた場合、その修理をどちらの国が行うのかという問題が発生する。また、B 国内において貨物に異常が生じていることが A 国にて発見された場合、誰がどのように対応するのかという問題も生じる。

次に、②のコストの問題だが、RFID のタグにも様々な種類があり、価格の幅も大きい。例えば、MATTS に使用するタグは1個1～2万円程度と高額であるが、EPCglobal で使用しているタグは1個数百円単位の比較的安価なものである。しかしながら、MATTS のタグはコンテナに貼り付けることを前提としているのに対し、EPCglobal では、カートン毎やパレット毎に貼付、それぞれに紐付けを行うことを目的としているため、MATTS よりも設置する個数が多くなり、コストが高くなる。MATTS の場合、保安に対する効果のみでは費用対効果のメリットが薄い。よって、保安対策の他に、物流効率化のメリットを享受することができないと、企業は導入しないと考えられる。

EPCglobal では、物流効率化が第一目的のため、今後は、セキュリティを目的とした MATTS と相互に協力してよりよいシステムを構築していくことも有益だと考えられる。

3.2 100%スキャニング法導入のための検討⁴⁾¹³⁾

100%スキャニング法とは、米国において2007年8月に成立した法律(the Implementing Recommendations of 9/11 Commission Act of 2007)であり、2012年7月1日以降、すべての米国向けコンテナについて、外国港湾においてX線やガンマ線を用いた透視検査及び放射性物質の検査を行うことを義務づけている。

ただし、実施にあたっては、下記の表-4の6つの条件のうち2つが該当する場合は、2012年までの期限を2年間ずつ延長する権限がDHSの長官に与えられている。

100%スキャニング法の実施にあたっては、図-1に示すように、米国向け貨物を船積みする港湾では、一次検査と二次検査が必要となる。

表-4 100%スキャニング法実施を延長できる条件

1) スキャンするシステムの購入・設置ができないこと。
2) システムの誤作動の率が高すぎる事。
3) スキャンするシステムの、海外の港における購入、導入、あるいは操作ができないこと。港湾がこのシステムを導入するための物理的な特徴を備えていないことも、そのようなケースに含まれる。
4) 既存のシステムと統合するのが不可能なこと。
5) システムの使用が、貿易能力と貨物の流れに重大な影響を与えること。
6) 疑わしい、あるいはハイリスクの貨物を自動的に通知する機能を十分に果たさないこと。

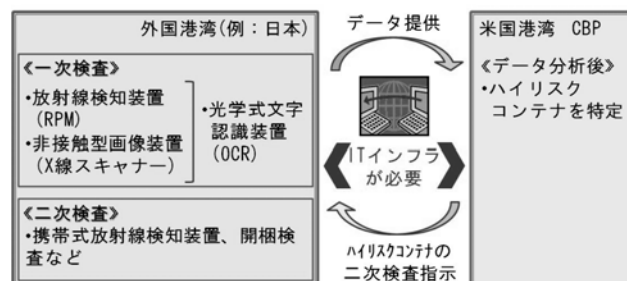


図-1 100%スキャニング法の概要

一次検査では「放射線検知装置」による放射線の検知と、X線やガンマ線による「非接触型画像装置」を用いたコンテナ内部の透視を行い、それらの検査で得たデータを米国のCBPへ提供する。CBPは提供されたデータの分析を行い、ハイリスクと特定されたコンテナについては、船積み前に二次検査を行うように指示する。二次検査が必要となった港湾では、ハイリスクと特定されたコンテナについて、「携帯放射線検知装置」を用いた再検査や、開扉検査などを行い、安全が確認された後でなければ船積みすることはできなくなる。

ここで、一次検査を実施する為に必要な設備は、下記のとおりである。

- ①放射線物質検知装置 (Radiation Portal Monitor : RPM)
- ②非接触型画像装置 (Non Intrusive Inspection System : NII)
- ③光学式文字読取装置 (Optical Character Reader : OCR)

米国としては、RPM、OCR、NIIを直線に配置し、その中をコンテナトラックが通過するドライブスルー型を提案している。

そこで、まず、日本においてドライブスルー型を導入して100%スキャニング法を実施する場合の問題点の検討を行う。

1) ドライブスルー型の問題点の把握

ドライブスルー型とは、ターミナルゲートに、

- ①放射線物質検知装置(RPM)
- ②光学式文字読取装置(OCR)
- ③非接触型画像装置(NII)

を順に設置し、ドライバーが停車することなくレーンを通り抜ける間に検査できるシステムを指す。

まず第一に、渋滞の問題である。ドライブスルー型を導入したとしても、都市部のコンテナターミナルにおいては、現在においてもゲート前混雑緩和のため、ゲート前にライブカメラを設置し、事前に混雑情報を提供しているターミナル（東京港：京浜港コンテナ輸送効率化検討委員会陸上輸送ワーキンググループの社会実験・横浜港：周辺で映像提供しているサイトを集めてある・博多港）もある。このような状況であるため、ゲート内外にて、さらに渋滞が発生する可能性が挙げられる。

第二に、ドライブスルーレーンのためのスペースの確保の問題が挙げられる。ドライブスルー方式を採用するには、放射線物質検知装置に影響を与えない間隔にて非破壊検査装置の設置を行わなければならないため、相当広いスペースの確保が必要になると想定される。

第三に、トランジット貨物の問題が挙げられる。トランジット貨物はターミナルのゲートを通過しないため、検査を行うことができない。

第四に、X線検査装置の使用に関する法的な問題が挙げられる。

日本においては、X線検査装置については、「放射性同位元素等による放射線障害の防止に関する法律」により、「使用施設の位置、構造及び設備が文部科学省令で定める技術上の基準に適合するものであること」が認められた場合のみ、文部科学大臣の使用の許可を受けることができる。「放射性同位元素等による放射線障害の防止に関する法律施行規則」によれば、使用施設の基準として、「文部科学大臣が定める線量限度以下とするために必要なしやへい壁その他のしやへい物を設けること」との記

述があり、屋外での使用を実施するには法改正が必要となる。

また、併せて「その室に人がみだりに入ることを防止するインターロックを設けること」との記述もあるため、運転手は下車し、X線検査装置使用場所とは別の部屋を通行する必要がある。

最後に、設置費用の問題が挙げられる。この100%スキャニングの法律は米国内の法律のため、諸外国の設備についても米国が費用負担することになると想定されるが、現時点では米国内において、予算措置ができていない。

2) ドライブスルー型の問題点解決のための検討

次に、これらの5つの問題を解決するために必要な事項についての検討を行う。

まず、一番目の交通渋滞の問題であるが、この解決には、現状を把握することが必要である。

よって、都市部の港湾の周辺交通量および、現状での渋滞発生状況を把握する必要がある。その後、モデルケースを作成するなどして、交通量に見合った必要レーン数を提案することが必要となってくる。

二番目のスペースの確保の問題については、X線検査装置をドライブスルーレーンとは別に配置する方法が考えられる。

現在、ドライブスルー型に配置するX線検査装置の他に、「移動式検査装置」と「CMS(Crane-Mounted Scanning)」があることが知られている。

移動式検査装置は、ターミナル内外を移動しながらスキャニングを行える車載式となっているため、新たに確保するスペースが不要である。また、CMSとは、ガントリークレーンに取り付けたスキャニング装置のことであり、船積みの際に検査ができるため、こちらの装置も新たに確保するスペースは不要である。

また、これらの装置を使用することにより、第三の問題点である、トランジット貨物の検査の問題も解決できる可能性がある。

船積み前のコンテナを移動式検査装置にて検査を行えば、ターミナルゲートを通らなくても検査することができる。また、CMSにて検査を行う場合は、船積みされるコンテナの全量を検査することができるため、こちらもトランジット貨物の検査も行うことができる。

ただし、この場合、一次検査の後、すぐに船積みされてしまうため、CBPから二次検査の指示が届いた際に、対象となるハイリスクコンテナが既に船積みされてしまっているという、新たな問題が発生する。

第四のX線検査装置の使用の法的問題については、法改正の必要性の検討と共に、使用機器による人体への安

全性の確認を行う必要がある。また、ドライブスルーレーンの必要数の検討により、ドライブスルーではなく、ドライバーが一度下車し、屋内にて検査を行うワンストップ式でも対応可能との結論が出れば解決できる。

五番目の設置費用の問題については引き続き米国の動向を把握するしかないが、費用を安価に抑える検討を行うておくことも必要であろう。費用を安価に抑えるには、既存の施設を活用することが第一である。X線検査装置については、日本においても税関が活用しており、全国に16箇所(13港)に配備している。よって、これらの施設を活用した導線の検討も必要である。

以上のことから、日本において100%スキャンニング法を実施するためには解決しなければならない問題が多々あることがわかった。

日本においてはこのような状況であるが、オランダはコンテナの100%スキャンニング法に応じる意欲があることを表明しており、ロッテルダム港においては自動コンテナ検査レーンについてもケーススタディが行われているとのことである。そして、ドライブスルー型自動コンテナ検査レーンについて、税関、港湾局、港湾業界とで共同で研究を行っているとの情報もある。

一方で、米国国内において、100%スキャンニング法の実施に関しては、諸外国港湾において100%スキャンニング法を実施できる港の整備が不十分であることを理由に懐疑的な声もあるとのことで、「米国における100%スキャンニング法実施の見通しについては、実施時期を延期せざるを得ない」と、2009年12月2日に開催された米国上院通商科学運輸委員会の「Transportation Security Challenges Post-9/11」にて、DHSのナポリターノ長官が述べたとのことである¹⁴⁾。

以上のことより、米国の今後の動向を見極めることが重要ではあるが、実際に100%スキャンニング法が実施された場合、EUなど他国においても同様の対策を実施する可能性も否定できないため、日本においても、オランダのような先進事例を参考に、対応策を検討しておくことが重要であろう。

4. その他のセキュリティ対策の検討

4.1 トレードリカバリープログラムの検討

2001年9月の米国同時多発テロ以降、米国を主導に各国・各国際機関において、テロを未然に防ぐための対策として、さまざまな取組を行っていることは先に述べた。これらの取組はすべてテロを未然に防止することが目的

である。しかしながら、テロを未然に防止する対策も必要であるが、仮にテロが発生した場合の対応策も重要である。その理由として、

- ①予防対策をすり抜けてテロが発生する可能性は否定できない。
- ②今まで以上の対策の強化は物流の効率化を阻害することになる。
- ③テロが発生した場合、世界経済に与える影響が大きい。ことが挙げられる。

テロが発生し世界の貿易が中断してしまった場合、経済に与える影響は甚大である。特に、貿易立国であるシンガポールでは貿易の中断による影響が大きい。よって、シンガポール政府は、テロにより貿易が中断した場合を考慮し、トレードリカバリープログラム TRP(Trade Recovery Program: 貿易復興計画)を提案し、APECにおいて検討しているとのことである。

このように、シンガポールが先導する専門家グループは、APEC全体に及ぶTRPの展開について研究している。これは、混乱を生じさせるような攻撃があった場合、可能な限り迅速に貿易を再開させるための原則や標準をもたらすことになると期待される¹⁵⁾。

また、米国においても有事の際は、C-TPATのTire3から貨物を通していくような検討も行われているとの情報もある。よって、日本においても、アジア諸国などと協力してTRPの策定に向けて検討していく必要があると考えられる。

4.2 セキュリティコストの現状

セキュリティのための費用の負担について見てみると、表-5のとおりISPSコード発効後、港湾管理者はISPSコードに対応するための費用カバーの目的で、船社に対し、Terminal Surchargeを課した。その後、船社がISPS tax Surchargeを導入し、荷主が費用負担を転嫁させられている。また、24時間ルール導入時も船社の準備対応投資の補填として、荷主にセキュリティ・チャージ、申告手数料が請求されている。その他にも、セキュリティプログラムによる企業への負担は監視カメラの設置等、目にみえる部分の費用のみではなく、セキュリティプログラムを実施するために、既存の業務プロセスを改正しなければならず、そのための費用もかかることになる。

表-5 セキュリティ規則によるサーチャージ

セキュリティ関連制度		徴収者	負担者	金額
ISPSコード	Terminal Surcharge	港湾管理者	船社	不明
	ISPS tax Surcharge	船社	荷主	\$6.00 Per Container or € 5.00 Per Container 程度
米国24時間ルール	AMS Surcharge	船社	荷主	\$25.00 ~ \$30.00 Per B/L
米国10+2ルール	申告手数料	フォワーダーなどの申告代理人	輸入者	\$10.00 ~ \$50.00 1申告当たり程度

5. 考察

現在では、まだ米国が主導してサプライチェーンセキュリティが実施されている現状である。

米国主導の対策は自国の保安対策を主としているため、米国への輸出を行う国々は費用の負担やリードタイムの長期化等の影響を蒙っている実情がある。さらに、テロを未然に防ぐためのこれ以上の対策の強化は貿易を阻害することにもなりかねない。

そこで、テロ発生を未然に防止する対策と同時に、万が一テロが発生した際の対応策を検討しておくことも重要である。いつ、どのような方法で起こるかかわからないテロ等を未然に防ぐ対策については限界もあり、また、各国において対策にかけられる費用の違いの問題もある。よって、今後さらなるテロ対策の強化に重点を置くよりも、荷主企業への負担をこれ以上かけない為にも、今後はTRPの策定も検討していく方が良いと考える。

なお、TRPの策定にあたっては、世界の物流を考慮して計画して行くことが重要と考えられる。現在では、世界各国にてAEO制度が浸透しつつあり、なおかつ相互認証への取組も進んでいる。よって、テロ発生時には、港湾の保安レベルの引き上げがなされるなどの対策が取られるが、その中でも、AEO制度の認証を受けている安全性の高い貨物から優先的に通関させるなどの、テロ発生後の速やかな貿易復興への対策へと重点が移行すると予測されるため、さらなる国際協力が必要となると考えられる。

一方で、RFIDなどの情報通信技術の進展に伴い、貨物のリアルタイム追跡技術が世界的に普及することも想定される。また、今後、100%スキャン法が実施される可能性もある。追跡技術が普及するには、システム全体を通しての責任の所在や費用の負担など、まだ解決しなければならない問題が残っており、100%スキャンにしても、物流を阻害することなく検査を行う方法についてまだ課題が残っている。

これらの問題の解決には、各々の問題を解決すること

はもちろん重要であるが、貨物のリアルタイム追跡が可能となり、コンテナの開封などの情報もリアルタイムで入手できるようになった場合、100%スキャン法については、すべてのコンテナを検査するのではなく、どこかで異常が生じたコンテナのみを行うなど、今後は対策相互の関係を整理し、現在別々に行っている対策を統合した対策とすることなどが求められてくると考えられる。

また、ISPSコードによる港湾保安対策は、現在までに海上コンテナを利用したテロが報告されていないことを考慮すると有効と考えられる。日本国内での法律の施行から5年が経過し、保安計画の見直し時期になっているため、今までの対策を再度見直し、死角の無い保安対策を心がけることが重要である。このような保安の確実性において信頼を得ることにより、ゆくゆくは港湾の国際競争力の強化につながると考えられる。

しかし、テロ対策に取り組むのは、物流の性質上、港湾だけの対策では不十分である。また、検査頻度を向上させると、物流の遅延も予測される。よって、オランダのように、関係する部署が協力して対策に取り組んでいくことが重要である。

6. まとめ

本資料では、サプライチェーンセキュリティの動向と日本の港湾にて対策を実施する場合の問題点について取りまとめた。

その結果、今後の日本の港湾の方向性としては、

- ・100%スキャンやRFIDを利用した貨物追跡システムの実用化の動向の見極めおよび、対応策の提案。
- ・TRPの提案。

を行っていくことが挙げられる。また、そのためにはまだ解決しなければならない問題が多いことがわかった。

また、米国は、まず最初にコンテナ貨物のセキュリティ強化の取組に重点を置いたが、今後はバルク貨物やLNG船などのセキュリティ強化の対策を行うことも想定される。

いずれにせよ、今後も世界の動向を見極め、適切な対応を図る必要がある。よって、今後も引き続き、保安対策の強化と物流効率化の両立化の手法を検討していく予定である。

(2010年3月16日受付)

謝 辞

本資料の作成にあたってはヒアリング調査において複数の保安関係専門家の方から御協力を頂きました。ここに謹んで謝意を表します。

参考文献

- 1) 経済協力開発機構(OECD):CONTAINER TRANSPORT SECURITY ACROSS MODES(2005)
- 2) 税関 HP (<http://www.customs.go.jp/>)
- 3) 日本機械輸出組合 HP (<http://www.jmcti.org/index.htm>)
- 4) (株)オーシャンコマース:荷主と輸送 2003年12月 P.3
- 5) 「米国における「10+2」(ノンマニフェストデータ)の提出が物流に及ぼす影響等」主催:(財)日本貿易関係手続簡易化協会
- 6) (財)運輸政策機構 HP (<http://www.jterc.or.jp/>)
- 7) Official Journal of the International Association of Ports and Harbors : Ports & Harbors September 2005 Vol.50 No.4
- 8) 国土交通省 HP (<http://www.mlit.go.jp/>)
- 9) (財)流通システム開発センター
HP(http://www.dsri.jp/epcgl/epc/about_epcglj.htm)
- 10) (株)オーシャンコマース:荷主と輸送 2009.11 No.421
- 11) (財)流通システム開発センター:電子タグ利用によるネットワークシステムの適用範囲の拡大研究調査報告書 2009年3月
- 12) Official Journal of the International Association of Ports and Harbors : Ports & Harbors July 2007 Vol.52 No.4
- 13) U.S. Customs and Border Protection : Report to Congress on Integrated Scanning System Pilots
- 14) WCO HP 2009/12/11 Press releases-2009 (<http://www.wcoomd.org/>)
- 15) Official Journal of the International Association of Ports and Harbors : Ports & Harbors July 2008 Vol.53 No.4

参考：英用語の略号

「10+2」 Rule (Importer Security Filing Additional Carrier Requirements)：輸入者セキュリティファイリングルール
100% Scanning：100%コンテナ貨物スキャンニング法
24-hour Advance Vessel Manifest Rule：積荷目録 24 時間事前通告規則
ABI(Automated Broker Interface)：自動通関申告システム
ACE(Automated Commercial Environment)：自動貿易流通システムー現在開発途中
ACS(Automated Commercial System)：電子通関システムの総称
AEO 制度(Authorized Economic Operator)：認可事業者制度
AIS(Automatic Identification System)：自動船舶識別装置
AMS(Automated Manifest System)：自動積荷目録システム
ATS(Automated Targeting System)：自動目標設定システム
CBP(U.S. Customs and Border Protection)：米国税関・国境警備局
CBRN 兵器：化学(Chemical)、生物(Biological)、放射性物質(Radiological)、核(Nuclear)兵器のこと
CSI(Container Security Initiative)：輸入海上コンテナ貨物のセキュリティプログラム
C-TPAT(Customs Trade Partnership Against Terrorism)：テロ行為防止のための税関・産業界パートナーシップ
DHS(Department of Homeland Security)：米国土安全保障省
DOE(Department of Energy)：米国エネルギー省
ISPS コード(International Ship and Port facility Security Code)：国際船舶および港湾施設の保安コード SOLAS 条約改正に伴い 2004 年 7 月 1 日に発効された国際規則
EPCglobal(Electronic Product Code global)：バーコードに代わるデータキャリアとして RFID とインターネットを利用した EPCglobal ネットワークシステムの開発・推進を行うために設立された非営利法人
MATTS(Marine Asset Tag Tracking System)：海上貨物追跡タグシステム
MI(Megaport Initiative)：核・放射性物質を検知するための巨大国際港湾におけるコンテナ・スキャンニング能力強化プログラム
NII(Non Intensive Inspection System)：非開封型画像装置
NVOCC(Non Vessel Operating Common Carrier)：非船舶運航業者
OCR(Optical Character Reader)：光学式文字読取装置
RPM(Radiation Portal Monitor)：放射線物質検知装置
RFID(Radio Frequency Identification)：電波による非接触型

自動認識技術

SFI(Secure Freight Initiative)：統合型スキャンニングシステムの検証のためのテストプログラム
SC(Supply Chain)：サプライチェーン
SCS(Supply Chain Security)：サプライチェーンセキュリティ
TRP(Trade Recovery Program)：貿易復興計画
WCO(World Customs Organization)：世界税関機構

国土技術政策総合研究所資料

TECHNICAL NOTE of NILIM

No. 585 March 2010

編集・発行 ©国土技術政策総合研究所

本資料の転載・複写のお問い合わせは

〔 〒239-0826 神奈川県横須賀市長瀬 3-1-1
管理調整部企画調整課 電話:046-844-5019 〕