ISSN 1346-7328
国総研資料 第528号
平 成 ２ １ 年 ３ 月

国土技術政策総合研究所資料

TECHNICAL NOTE of
National Institute for Land and Infrastructure Management

No. 528 March 2009

海上輸送を中心とした最近のサプライチェイン セキュリティの動向

岩瀬美奈子・安部智久・関裕・宮地豊

Recent Development of Supply Chain Security Related to Maritime Transport

Minako IWASE,Motohisa ABE,Yutaka SEKI,Yutaka MIYAJI

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

国土技術政策総合研究所資料
No.528　2009 年 3 月
(YSK-N-185)

海上輸送を中心とした最近のサプライチェイン セキュリティの動向

岩瀬美奈子*・安部智久　・関裕***・宮地豊****

要　　旨

企業がサプライチェイ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 条約における ISPS コードによる保安対策に加え，サプライチェイン全体についての保安対策も進みつつあり，これは保安を含む港湾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海上輸送保安対策（サプライチェインセキュリティ）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：　サプライチェインセキュリティ，AEO , ISO28000, WCO

＊　　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
＊＊＊　関東地方整備局　港湾空港部
＊＊＊＊管理調整部　部長
〒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

Technical Note of NILIM
No. 528 March 2009
（YSK-N-185)

Recent Development of Supply Chain Security Related to Maritime Transport

Minako IWASE*
Motohisa ABE*
Yutaka SEKI **
Yutaka MIYAJI ***

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, ISO28000, WCO

* 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 Port and Airport, Kanto Regaional Office, MLIT
*** Dept. of Administration and Coordination, NILIM

目　　次

1. はじめに

2001年9月11日に発生した米国同時多発テロ事件を契機として，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．これにいち早く対応したのは IMO *(International Maritime Organization : 国際海事機関)であり，港湾施設と船舶における保安対策強化のための改正SOLAS 条約が 2004 年 7 月に発効され，我が国でも「国際航海船舶及び国際港湾施設の保安確保等に関する法律」を施行し，国際港湾施設における保安措置を実施しているところである．

しかし港湾・海上輸送はサプライチェイン（Supply Chain）の一部に過ぎないことから，各国は国際輸送におけるこれ以外の部分，ないしはサプライチェイン全体における保安対策（Supply Chain Security : サプライチェインセキュリティ）を強化する動きにある．

例えば米国では，2003 年に DHS（Department of Homeland Security : 国土安全保障省）を設置し，テロ攻撃の再発防止に努めており，輸入貨物に紛れてテロリスト，CBRN 兵器等が米国内に流入してくるのを防ぐ目的でいくつもの対策を打ち出し，コンテナ貨物輸送に関連したサプライチェイン全体でのセキュリティ強化対策に取り組んでいる．

米国の取組に続いて EU，他の国際機関においても，国際サプライチェインにおける安全性確保の取組を実施している．一方我が国においても平成 20 年の関税法の一部改正が行われ，日本の AEO(Authorized Economic Operator)制度となる新たな認定通関業者制度が導入された．

サプライチェインセキュリティの強化は，荷主や海運事業者等の物流活動に多大な影響を及ぼす．例えば米国による米国への輸出国の積出港において危険を阻止しようとする対策は，荷主企業の貿易に係る費用の増大やリードタイム増加等の物流の効率性を著しく低下させる可能性がある．

また，世界的にサプライチェインセキュリティが進む中で，我が国における対応が遅れれば，我が国発の貨物に対して信頼性が低下し，輸出先国での貨物検査率の上昇など，荷主に対して不利益が発生する可能性がある．

さらには，国際輸送における保安対策に関しては一国のみによる取り組みでは限界があり，日本以外の各国との適切な連携を図る必要がある．

以上のことから，我が国においても急速に進展しつつあるサプライチェインセキュリティの世界的動向を把握した上で，港湾を含むサプライチェインを構成する企業全体が官民の連携の下適切な対応を取る必要性が生じている．

本資料は，港湾運営等にかかわる主体が今後の保安対策への適切な方策を考える上での基礎資料を提供する観点から，各国，国際機関の取組内容の現状を把握し，今後の予測される海事輸送を中心としたサプライチェインの保安対策の動向ならびに今後の港湾への影響等について整理を行うものである．2 章でサプライチェインセキュリティの概要について述べ，3 章で主要国・国際機関の対策の現状，4 章においてサプライチェインセキュリティの今後予測される動向や今後の港湾への影響等について考察を行う．

2. サプライチェインセキュリティの概要

国際輸送保安対策の概要については，経済協力開発機構（OECD）の「CONTAINER TRANSPORT SECURITY ACROSS MODES(2005)」[1)]が詳しく，サプライチェインセキュリティを確保する方法として下記の5項目を挙げている．

①コンテナの内容物の物理的検査（スキャニング）
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

コンテナ貨物を利用したテロの脅威には，「ハイジャック」型と「トロイの木馬」型の大きく二つに分類される[1)]．「ハイジャック型」とは貨物を奪うことであり，また「トロイの木馬型」はサプライチェインの起点である荷主や混載業者等がテロリストに支配されてコンテナが輸送される，コンテナの不正使用（なりすまし）である．この二つの脅威のパターンへの対策は異なる．

以下に各々の対策の考え方を示す．

1）コンテナ内容物の物理的検査（スキャニング）

内容物の物理的検査の方法は，X 線スキャナなどの非開扉検査(NII)装置でコンテナをスキャンし，内容物を識別する方法と，コンテナを開き手作業で船荷証券と一致させる方法の 2 種類がある．

コンテナを開梱する方法は貨物の流れに遅延を生じてしまう．このため遅延を最小限にとどめるため非開扉検査が用いられているが，非開扉検査は，検査が可能なターミナル区域の制約，機械の費用，オペレータの人員確保等の問題を伴い実施しているのは一般的に輸入コンテナの場合で数%程度である．

「トロイの木馬（なりすまし：コンテナの不正使用）」の場合，コンテナのハイジャックや改ざんと異なりコン

*英用語の略号は巻末に一覧を掲載する

テナは表面的には合法とみなされることから，唯一の対策は物理的検査（スキャニング）のみとなる．

コンテナ内容物のスキャニングは，効果的なセキュリティ対策であると同時に，高価で煩雑な対策であり，多くの貨物のスキャニングは費用や時間等の関係上難しい．このためこれを補完するため，事前に入手できる情報に基づきセキュリティリスクの評価を行い，ハイリスクコンテナを識別するスクリーニングが必要となる．また，非開扉検査技術の研究開発やスキャニングの対象となるハイリスクコンテナを識別するためのスクリーニング技術の確立が重要である．

2）コンテナの保全性（シール技術）の確保

輸送途中でコンテナ内容物を出したり，内容物を入れ替えたりといった改ざん防止のため，コンテナの保全性の確保はコンテナセキュリティの確保の基礎となる．

一般的なコンテナは，片方の端にある両面ドア１箇所で閉じる構造となっているため，このドアが不正に開封されないよう保全性を保つための密封装置として，メカニカルシールや電子シールが使用される．

メカニカルシールとは，コンテナの密封を示す装置でありコンテナが開封された場合，シールそのものが破壊して改ざんを知らせるものであるが，同じようなシールに交換すればコンテナ内容物の改ざんはわからない．

このため現在では，自律した電源が組み込まれており，継続して信号を記録しデータを遠距離送信することができる電子シールが開発されている．

電子シールは国際輸送全体で使用できるものでなければならないが，異なるメーカーが互換性の無いシステムを開発しているのが現状であったため，サプライチェイン全体で使用可能な国際規格が国際標準化機構（ISO）によりISO18185（海上輸送コンテナ用の電子シール）として公表されている．

また，コンテナ内部の環境条件を追跡する多機能センサーを搭載するスマートコンテナの開発も進められており，たとえばコンテナ内部の温度の上昇や衝撃を監視することで不正な開封を把握することができる．

3）コンテナ輸送環境の保全

コンテナの輸送環境を保全し，コンテナの不正開封や不正物の混入を防ぐことが必要である．その手段として，物流関係施設への出入り管理（アクセスコントロール）やCCTVによる監視体制の強化等がある．

一般に，コンテナの移動中のリスクは少なく，積み替え地点のターミナル施設等においてコンテナの改ざんやハイジャックの可能性が高い．よって，サプライチェイン全体の関係者間で輸送ノードにおけるコンテナ輸送環境の保全性を確保するための共通の指針，作業手続き，研修プログラム等を整備し，信頼性を向上させることが必要である．

4）コンテナの追跡

コンテナがハイジャックされるなど輸送に異常が生じた場合，予定された輸送ルートを外れるなどの事態が生じる．このためコンテナを追跡することにより，ハイジャックされたコンテナを早期に発見できる可能性がある．

コンテナを追跡する方法としては，「輸送の要所において確認を行う方法」と「連続したリアルタイム追跡」の２つの方法がある．コンテナ追跡は必ずしもリアルタイムである必要は無いが，異常事態を検知した際に対応が手遅れとならない適切な時間間隔及び場所のデータでなければならない．港湾などの複数の輸送モード間の結節点などにおいてコンテナが追跡できるシステムを導入することが必要である．

5）貿易文書及び輸出入貨物情報の管理

最も確実な保安対策は実際に貨物をスキャニングすることである．しかしすべてのコンテナが同じリスクではなく，コンテナの貿易は繰り返しが多く，また大手荷主によるものは同じ内容（品目，貿易国等）の繰り返しである場合が多いことから，このような貿易に関する文書及び貨物情報を適切に管理・分析することでスキャニングの効率を向上させることができる．例えば，税関によって保安上のリスクが低いと判断された認可業者（AEO）による貿易である場合は，貨物のスキャニングを行う頻度を減ずることが可能となる．

このような貿易上の情報の管理・分析においては国際サプライチェインにおける輸出国から輸入国の税関に至るまでのコンテナのスクリーニングに取得・使用するデータの内容や用途，情報提供の時期，機密性保持について整合性を保つことが重要である．また，起点の船・荷主から最終の受取人まで積荷を追跡し，コンテナ積荷のスクリーニングを担当する主要な機関に必要な情報を提供できるシステムの開発が必要である．

6）サプライチェインセキュリティ

以上の１）～５）を組み合わせた，サプライチェイン全体での輸送保安対策（サプライチェインセキュリティ）の概要を**図-1**に示す。左側に輸出国（例えば日本），海上輸送を挟んで右側に輸入国（例えば米国）を示している．

各物流施設においては，コンテナの取り扱いに関連した施設のアクセス管理（関係者以外の当該施設への出入りの禁止やCCTV等による監視体制を強化等）により，コンテナへの不正アクセスを防止する．いったん閉じられたコンテナについては，コンテナシールの利用により

不正な開封を管理する．電子シールやスマートコンテナを活用することで，不正な開封や異常事態（温度上昇や衝撃等）が発生した場合の早期における検知を行う．

陸上輸送中においても，リアルタイムないしはそれに近い形で貨物輸送経路の追跡を行うことで，コンテナの異常（ハイジャックによる予定経路からのずれや不正な開封等）の早期発見が可能となる．コンテナの追跡や電子シールによる輸送状況の管理をリアルタイムで行うためにはトランシーバーや GPS，RFID といった情報通信機器の活用が必要となる．

大口荷主によるコンテナ（FCL）の場合のみでなく，小口荷主による混載（LCL）貨物についても，アクセス管理等の対策が必要となる．

港湾及び船舶については，既に ISPS コードによる保安対策により，港湾についてはコンテナターミナル内の制限区域の設定とアクセス管理，船舶についてもアクセス管理や異常事態発生時の対応等が実施されている．

これらとは別に，水際対策としての貨物検査が税関を中心に実施される．具体的にはコンテナ開封や非破壊検査（X 線等）が行われるが，100%の検査には時間とコストを要するため，通常は事前の貨物情報を荷主や船会社などに提出させることにより，検査すべきコンテナが特定される．これは輸出の場合と輸入の場合の両者に当てはまり，貨物が到着し検査が行われる前に必要とされる貨物情報が検査当局によって入手され，かつ適切な貨物のリスク評価（スクリーニング）がなされることで検査すべきコンテナが特定されることが必要である．また，特定の大口荷主により繰り返し輸出入される貨物や，一定の保安対策がなされ，かつ法令遵守が確実である荷主等の認可事業者（AEO）による貨物については，このような検査の率を減少させ，不要な検査を極力防止することが必要である．

コンテナが輸入国側に到着した後も，施設のアクセス管理や貨物の追跡等について輸出国と同様の保安対策が継続される．

このように，１）から５）までの対策を組み合わせかつサプライチェイン全体で保安対策を講ずることがサプライチェインセキュリティの基本的考え方である．

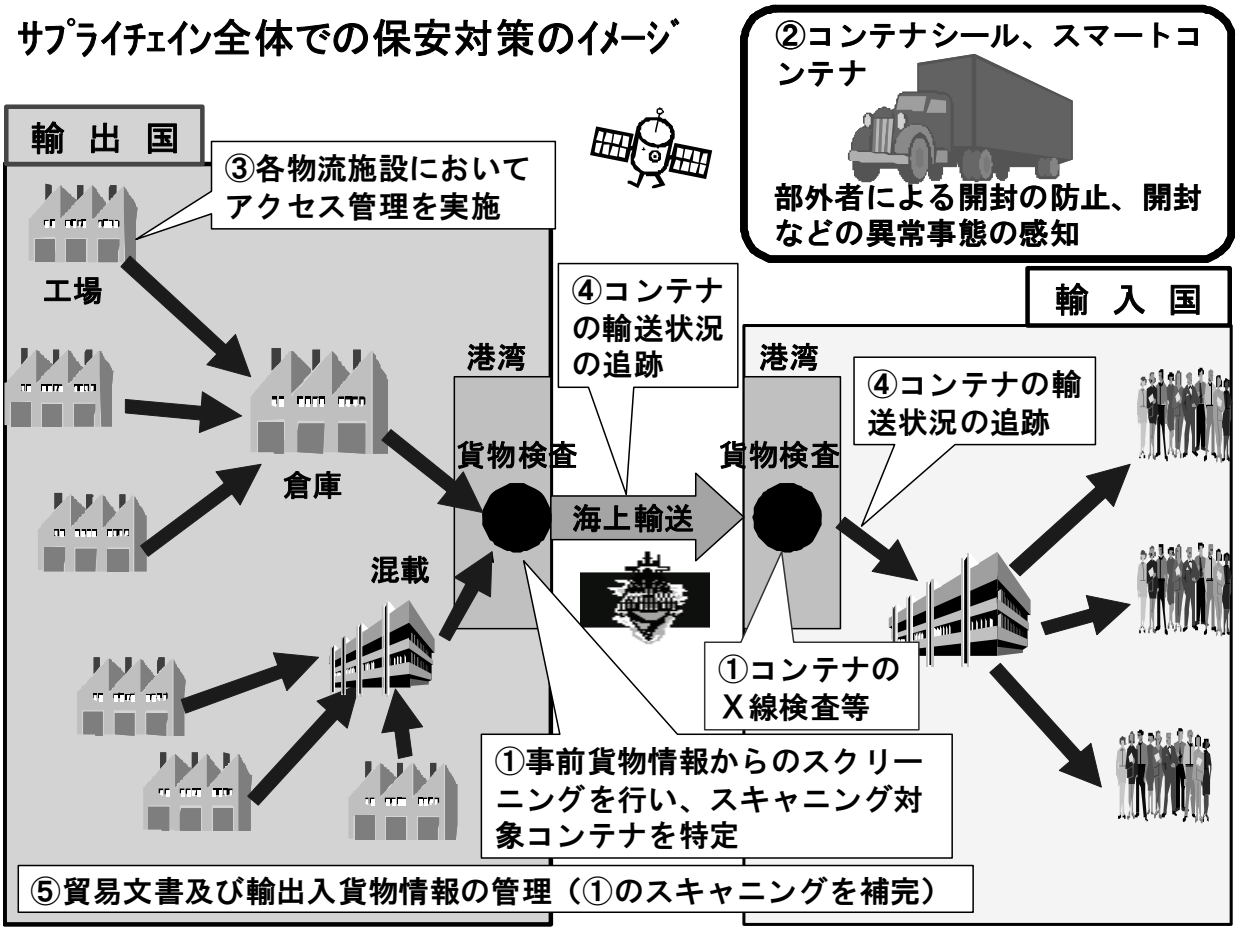

図-1 サプライチェイン全体での輸送保安対策の概要

３．各国・国際機関の対策の現状

本章では，各国や国際機関等において実際に検討されているないしは実施されている対策の現状を紹介する．

3.1 米国における対策と現状

米国では，2001 年のテロ事件以降，様々な国際輸送に関するセキュリティ対策を打ち出しているが，ここでは代表的な対策の現状を述べる．

１）CSI(Container Security Initiative) [2)3)17)18)19)]

外国港湾において，コンテナが米国向け船舶へ積み込まれる前に安全保障上のリスクがある海上コンテナを特定，調査・発見するためのプログラムである．

テロリスト，あるいは大量破壊兵器の米国内流入を阻止するための第一線を，港湾・空港を含む米国国境から，海外の出発・出航地点へ拡張するという米国政府の安全保障政策に基づいた制度であり，コンテナ貨物に対するセキュリティを強化した対策 [17)]である．CSI の内容に関する基本的要素を**表-1** に示す．

表-1　CSI の基本的要素

1）ハイリスク･コンテナのリスク基準策定
2）米国港湾到着前の事前検査の実施
3）ハイリスク･コンテナを検査するための機器の開発
4）より高性能で安全性の高いコンテナの開発と使用

CSI は，2002 年 1 月 17 日に DHS(Department of Homeland Security：国土安全保障省)所管の CBP(U.S.Customs and Border Protection : 米国税関・国境警備局)により発表され，その後，SAFE Port Act 2006 で法制化された米国と対象港との 2 国間政府レベルでの協定によるセキュリティプログラムである．対象となる港は，第 1 段階として，米国へのコンテナ輸出量が最も多い港から第 20 位までの港，第 2 段階として，その他の比較的中小規模の外国の港とし，CBP の専門官の派遣を行い，コンテナ貨物の検査を実施している．**表-3** に CSI 港湾に必要な最低基準を，**表-4** に CSI 港湾として求められる環境を示す．我が国では，**表-2** に示すように，2003 年 3 月に横浜港で導入され，その後，東京港，神戸港及び名古屋港において導入されている．CSI は相互主義に基づいていることから，上記の 4 港において CBP の専門官を受け入れるとともに，我が国からもロサンゼルス港，ロングビーチ港へ職員を派遣し，実施している．

CSI 港湾では，米国への輸出港を出る段階で近代的機材（X線，ガンマ線検査装置）によるコンテナ検査を行い，ローリスクコンテナとハイリスクコンテナに分別し，同時に貨物のマニフェストが米国側へ送られる．該当コンテナが米国に到着した時に，既に送られているマニフェストと照合することで米国に到着したローリスクコンテナは，ファーストレーンに乗せられ，迅速な輸入通関が行われる．よって，通常 CSI 実施港のコンテナは CSI を実施していない港から輸送されたコンテナよりも迅速に陸揚げ許可が与えられる．24 時間ルール（次項）に基づき，米国税関に対して輸出港での船積み 24 時間前に申告される情報を米国の税関の検査官が検査し，輸出国の税関からの情報と付き合わせることで輸出段階でのハイリスクコンテナの特定も行っている．

2008 年 5 月現在で 58 の港で実施中であり，米国向けに出荷されるコンテナ貨物のおよそ 85%をカバーしている [2)]．

表-2　CSI 導入の履歴

2002年 1月	CSI計画発表
2002年 2月	オランダ(ロッテルダム港)が最初に導入
2003年 3月	横浜港導入
2004年 5月	東京港導入
2004年 8月	神戸及び名古屋港導入
2006年10月	SAFE Port Act 2006制定

表-3　CSI 港湾に必要な最低基準

1）米国内の他港に、ある一定量以上のコンテナを定期的かつ直接輸送する
2）当該港湾の税関はコンテナの積載地や積み替え地、出港地を検査できる
3）ガンマ線かX線、あるいは放射線によるコンテナ検査装置を備えている

表-4　CSI 港湾として求められる環境

1）自動リスク管理システムを導入している
2）重要なデータや安全保障上の情報や諜報活動を国土安全保障省(DHS)の税関･国境警備局(CBP)と共有できる
3）港湾環境の評価を実施し、基幹構造上の脆弱性を認識し、解決できる
4）すべての規制に準拠し、基準を満たせない部分があるならばそれが何かを突き止め、改善できる

２）24 時間ルール

（24-hour Advance Vessel Manifest Rule）[2)3)17)18)19)]

税関が早期に米国に到着する貨物をスクリーニングしリスクを把握すること，またそれにより貨物の流れを円滑にすることを目的にした規則である．

表-5 に示す通り，2002 年 12 月 2 日に「積荷目録 24 時間前事前通告規則」が施行され，外国港湾で船積される米国向け貨物は，「貨物情報」及び「米国通過非米国貨物情報」を船積 24 時間前までに船社や NVOCC が CBP に対して AMS（Automated Manifest System）を通じ電子的に事

前申告することが義務づけられた．申告する内容については**表-6** の通りである．24 時間ルールに基づき義務づけられている情報が CBP に対して提出されない場合は**表-7** の罰則規定が適用される．

貨物積込 24 時間前までに船社等が CBP へ貨物情報等を申告するためには，荷主はさらに 24～72 時間前に貨物情報を船社に提出することが必要となり，規則施行前よりも輸送リードタイムが数日長期化するという影響が生じている．また，船社はコンテナを出港の 2～3 日前に受け取らなければならなくなり，コンテナヤード内での滞留した輸出コンテナ貨物による混雑が問題となっている．また荷主に対しては輸送リードタイム増加による保有在庫の増加やコンテナヤードの蔵置期間増に伴う費用増加が生じている．ただし 24 時間ルールに関しては，実施から数年が経過し，すでに米国向け貨物を取り扱う事業者の中では定着してきている．

米国以外の各国でも，貨物のスクリーニング強化のための貨物情報の事前申告の重要性が認識されており，**表-8** に示す通り法制化され，EU においても 2009 年 7 月 1 日から実施予定である．しかし申告の対象となる貨物及びその期限について国際的に整合性が保たれていないのが現状である．この他，中国においても 2009 年 1 月 1 日から中国向け貨物の情報を船積み 24 時間前までに電子申告する 24 時間ルールを導入している．

表-5　24 時間ルール導入の経緯

2002年12月	「積荷目録24時間事前通告規則」施行 (24-hour Advance Vessel Manifest Rule) ◇ 米国向け海上貨物が対象
2004年 1月	「貨物情報の早期かつ電子的提出に関する規則」施行 ◇ 海上輸送に限定されず、航空・陸上貨物まで範囲が広がる

表-6　24 時間ルール申告事項

① 米国向け船舶が出港した最後の港
② キャリアコード
③ キャリアの航海番号
④ 最初の米国の寄港地への到着予定日
⑤ キャリアの航海番号B/L番号と数量
⑥ 米国行き外国キャリアが最初に貨物を受け取る港名
⑦ 貨物の正確な説明(6桁のHSコード)と重量、またはシールされたコンテナについては荷主が申告する貨物の説明と重量 (総称的説明は認められない)
⑧ B/L記載の荷主の完全な名前と住所
⑨ B/L記載の荷受け人の名前と住所
⑩ 船舶名、ドキュメントの作成国、及び公式船舶番号
⑪ 貨物の積み込みが行われた外国港名
⑫ 国際的に認識された危険物質コード
⑬ コンテナ番号
⑭ コンテナに添付されているシール番号

表-7　24 時間ルールの罰則規定

・ 外国における貨物の積載を禁止
・ 米国の港における貨物の陸揚げ等を禁止
・ 違反行為に対して、最初は5,000ドル、2回目以降は10,000ドルの罰金を科すことができる。

表-8　各国・機関の事前申告ルール

		米国	日本	WCO	EU
法令	根拠となる法令	2002年通商法 Trade Act of 2002	関税法	SAFE「基準の枠組み」	関税法
	事前申告実施時期	2002年12月2日施行	2007年2月1日施行	2007年6月	2009年7月1日　発効予定
輸入貨物	コンテナ貨物	輸出国の港での積込の24時間前	日本の港へ入港する24時間前	出発地における荷詰めの24時間前を限度	輸出国の港での積込の24時間前
	バルク貨物	米国到着の24時間前	日本の港へ入港する24時間前	仕向地の最初の港に到着する24時間前を限度	EU税関領域到着の24時間前
輸出貨物	コンテナ貨物	出帆24時間前※	－	出発地における荷詰めの24時間前を限度	積込24時間前
	バルク貨物	出帆24時間前※	－	仕向地の最初の港に到着する24時間前を限度	EU税関領域から運び出される24時間前

※米国輸出貨物については2008年7月2日発効、2008年9月30日より実施。

３）C-TPAT

(Customs Trade Partnership Against Terrorism) [2)3)17)18)19)]

輸入業，仲介業，運送業及び国外の製造業などすべての構成者間における連携を密にすることで，それぞれの企業がサプライチェイン上における保安対策を強固なものにすることを目的とした制度である．

2001 年の米国同時多発テロ事件後，326 箇所の米国の空港，海港，指定された陸上国境を通過する貨物を通じたテロ攻撃の可能性を抑制するために制定された，セキュリティ強化と貿易円滑化の両立を図るための官民共同の自主的な取組であり，2002 年 4 月に導入され，SAFE Port Act 2006 の中で法制化された．

C-TPAT の参加企業は，階層 1(Tier Ⅰ)，階層 2(Tier Ⅱ)，階層 3(TierⅢ)と，3 段階に区分され，**表-9** に示す通り階層に応じて適格要件及び，通関上の優遇措置が異なる．

階層 1 に参加するためには**表-10** に示す最低要件を企業自身が診断・評価を行い，**図-2** に示すように参加同意書等を提出すると，CBP が内容を審査し，認定行為が行われる（certify）．階層 2 に参加するためには，更に CBP による実地調査（validation）を行い，一定の基準を満たしている事を証明することが必要となる．階層 3 は，階層 2 参加者認証用に設定された指針を越えるセキュリティ対策の維持に対する継続的な努力を立証した参加企業にのみ与えられる．

税関の無条件通過が与えられるのは階層 3 の認証を受けた企業だけになる見込みであり，審査は厳しく，2008 年春の時点で約 250 社である [20)]．

表-9　C-TPAT の取得状況

	Tier Ⅰ	TierⅡ	TierⅢ
優遇措置	・ ATS※に基づいて割当られたリスク点数を20%を越えない範囲で減点	・ ATSに基づき割り当てられたリスク点数の減点 ・ 貨物検査の縮小 ・ 貨物の優先調査	・ 長官の指定する全脅威レベル中の米国内仕向港でのTierⅢ参加者貨物の速やかな開放 ・ 貨物検査の更なる縮小 ・ 貨物検査の優先性 ・ ATSに基づき割当られたリスク点数の更なる減点 ・ 適宜、合同事故管理演習への加入
取得方法	自社のサプライチェーンのリスク分析を実施済みで、脆弱性を減らすための対策をすでに講じたという証明書を税関に提出すれば取得できる。 認定(Certified)を受けた事業者。	税関に提出した証明書の有効性を、税関職員が認証することで与えられる。 実地調査(Validation)を受けた事業者。	CBPが定めるサプライチェーンのセキュリティに関するベスト・プラクティスに従っていると判断された企業に対してのみ付与。
参加会社数	2008年春の時点で8,000社以上	2006年春の時点で1,500社以上が取得済みで約2,300社が申請中	2008年春の時点で約250社

※ATS:(Automated Targeting System:自動検知システム)米国向け貨物の100パーセントを綿密にスクリーニングを行うシステム。詳細は明らかにされていないが，申告情報の諸項目にポイントを割当てるシステム。

① C-TPAT参加同意書に署名
② CBPのガイドラインに基づき、自社の物流に関する安全保障措置に関し、**自己審査**
③ CBPに自社の安全保障措置内容の説明書を提出

⇩ CBP；物流の安全保障確保の為に適切な体制を整え必要な措置を講じていると認める

C-TPATの参加会社として正式に認証を行う

※参加後も、厳格に物流安全保障のための自己管理が行われているかどうかを確認するため、CBPの担当者が参加会社の代表を面接したり、参加会社の現場を視察することがある。
（＝Validation Process）

図-2　C-TPAT 参加手続きの概要

表-10　参加最低要件

1）国際サプライチェーンにおける貨物移送実績の立証
2）コミッショナー（最高責任者）を通じて職務をとる長官が設定した以下に記載する(A)～(G)等のセキュリティー基準に基づいた、そのサプライチェーンの評価 (A) ビジネスパートナー要件 (B) コンテナセキュリティー (C) 物理的セキュリティー及びアクセス管理 (D) 職員のセキュリティー (E) 手続き上のセキュリティー (F) セキュリティー訓練及び警戒認識 (G) 情報技術セキュリティー
3）セキュリティー対策とコミッショナーが定めたセキュリティー基準にかなったサプライチェーンセキュリティー慣行の実施と維持
4）通商活動諮問委員会と協議して、コミッショナーが設定したその他すべての要件の充足

4）ACE(Automated Commercial Environment)[5)6)]

ACE とは，米国の通関等の各種貿易関係省庁システムのシングル・ウィンドウ化を目的とした CBP の運営する貿易通関電子システムの総称であり，2011 年までに完成予定とされているシステム[15)]である．

現在米国では，ACS（Automated Commercial System：電子通関システムの総称）が使用されている．このシステムは輸入貨物の通関に関するシステムであり，輸出については別に AES（Automated Export System：自動輸出手続きシステム）が利用されている．ACS の中には，AMS（Automated Manifest System：自動積荷目録システム）と ABI（Automated Broker Interface：自動通関申告システム）が含まれており，24 時間ルールでは，事前マニフェスト情報を AMS により申告することが義務付けられている．ACE が開発されれば，税関職員を始めとする輸出入に関連するすべての政府機関窓口及び，輸出入に係る通関業や運送業等の民間企業全てが同じシステムに参加することにより，現行の ACS の通関業務に加えて，サプライチェイン全体での情報を得られるようになる．今後，ACE が開発・実用化されれば，このシステムを通じて税関職員は貨物に関するこれらのデータを取得し，貨物の事前スクリーニングをより効率的に行うことが可能となる．

また，ACE については 2003 年からテストが実施されており，当初のフェーズⅠでは，C-TPAT 参加者に限定して，40 社による試験が実施されている[5)]．

5）MI(Megaport Initiative)[4)14)15)16)]

MI とは，2003 年から開始された DOE（Department of Energy：米国エネルギー省）のプログラムであり，テロリストによるコンテナの不正使用による核・放射性物質の不正取引防止や，核拡散防止の観点から，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・スキャニング能力強化を目的としている．

2008 年 5 月時点でアメリカ政府は 27 ヶ国・地域との間で実施合意を結び，オランダ，ギリシャ，バハマ，スリランカ，シンガポール，スペイン，フィリピン，ベルギー及びイスラエルの 9 ヶ国において，メガポート・イニシアチブを実施している．

我が国においても，2008 年 7 月に米国との間でメガポート・イニシアチブのパイロットプロジェクトを実施することに合意しており，2009 年 3 月を目標に，横浜港（南本牧ふ頭）において実証実験を開始できるよう，外務省・財務省・国土交通省が連携し，準備を進めているところであり 1 月には検査機器が設置された．

我が国での MI のパイロットプロジェクトのイメージを参考に図-3 に示す．

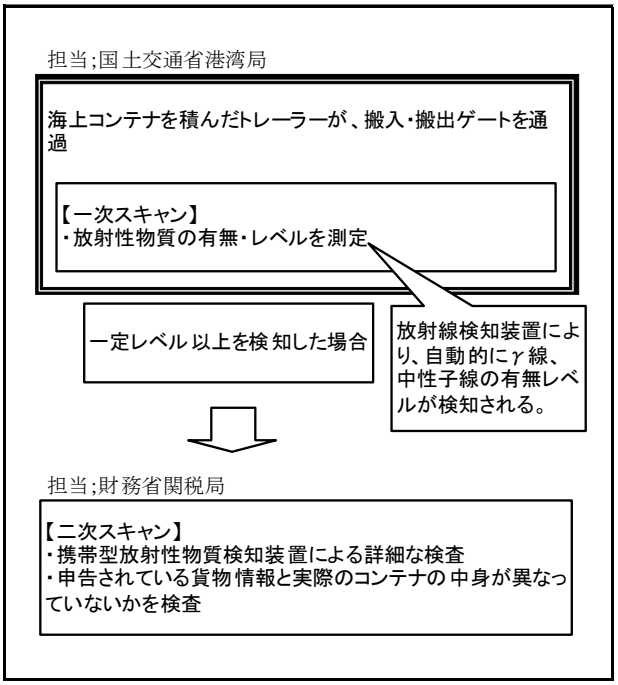

図-3　MI イメージ[16)]

6）SFI(Secure Freight Initiative)[4)17)18)]

SFI とは，「統合型スキャニング・システムの実行の可能性を検証するためのテストプログラム」と呼ばれるイニシアチブであり，2006 年 12 月に発表された．海外における核物質及び放射能物質のコンテナをスキャンするため，そして，到着コンテナのリスクをより正確に判断するためのシステム機能をさらに高めることを目的としている．DHS の CSI と DOE の MI の対策を統合し，実際の運用は DHS 傘下の CBP が行うというものである．

SFI のテストプログラムは，第 1 段階及び第 2 段階が行われており，テスト内容，テスト実施港及びテスト目的は表-11, 12 の通りである．SFI は後述する 100%スキャニ

ングの実現の可能性をテストするプロジェクトとなっていることが特徴である．

表-11　目的とするテスト内容

① 全ての米国向けコンテナのスキャニング
② 画像および情報の米国への送信
③ 放射性物質検知装置がアラームを発した場合の対応方法

表-12　テスト実施港及びテスト目的

＜第1段階＞	
目 的 ：	コンテナの船積前全量検査 新体制がロジスティクス、港湾業務、貿易の流れにどのようにスムーズに統合できるかについて、証拠を提供する段階
テストプログラム実施港	
英国	サザンプトン港
パキスタン	カシム港
ホンデュラス	プエルト コルテス港
＜第2段階＞	
目 的 ：	貨物情報の到着前審査 当該貨物の国際輸送に関わるサプライチェーンの全ての関係者から、商業取引情報を第三者機関が収集・集計し、それを基にDHSがリスク分析を行い、検査の必要性或いは国内持込禁止の判定を行う。
テストプログラム実施港	
香港	モダン ターミナル
韓国	ガンマン ターミナル
シンガポール	ブラニ ターミナル
オマーン	サララ港

7）MATTS(Marine Asset Tag Tracking System)[16)]

MATTS とは，DHS の総合的な貨物安全戦略の一部として開発が進められている海上貨物追跡タグシステムである．海上コンテナに GPS 機能が付いた IC タグを取り付け，地球規模での通信及び追跡を遠隔操作により可能にするものであり，コンテナの位置情報やドアの開閉などのセキュリティ情報をリアルタイムで監視することのできるシステムを目指している．

我が国においては，日米科学技術協力協定における日米安全安心科学技術協力イニシアチブのもと，DHS の要請に基づき国土交通省港湾局が支援し，平成 19 年，平成 20 年に実証実験を実施している．

平成 19 年度は基礎的な輸送実証実験として，100 個の MATTS 通信機器を日本から米国への港間を輸送されるコンテナに取り付けて実施した．平成 20 年度ではサプライチェインへの適用をより重視し，日本国内の工場から米国内陸部の工場までの追跡実験を行っているところである．

8）100％スキャニング（100%Scanning）[7)17)18)]

100％スキャニングとは 2007 年 8 月に成立した法律(the Implementing Recommendations of 9/11 Commission Act of 2007)に基づき，2012 年 7 月 1 日以降，すべてのアメリカ向けコンテナについて，外国港湾において X 線による検査及び放射性物質の検査を行うことを義務づけた法律である．SFI において 100％スキャニングのパイロットプロジェクトを実施中であるがその実現可能性について結論が出ていないにも関わらず成立した法律である．

100％スキャニングの大きな問題としては，検査にかかる時間と検査場所及び検査にかかる費用（検査のための機器や人員等）などが挙げられる．

検査にかかる時間については，使用する画像システムによって検査処理時間に差が出ることが，SFI のパイロットプロジェクトの結果から判明している．

CBP が米国議会へ提出した報告 Report to Congress on Integrated Scanning System Pilots[7)]によれば，スキャニングにあたっては，RPM(Radiation Portal Monitor : 放射線物質検知装置)，OCR(Optical Character Reader : 光学式文字読取装置)，NII(Non Inteusive Inspection System : 非開封検査装置)が必要となる．物流の流れを阻害せずにこれらの検査を実施しようとした場合，ドライブスルー型を採用することとなり，広範なスペースを確保することが必要となる．またドライブスルー型装置の使用については運転手が乗車したままの検査になることから，健康上（放射能被ばく）の問題から禁止している国・政府が多いとの指摘がされている．

また，DHS と日本機械輸出組合との意見交換会[17)]においても，スキャニング機材の整備にかかる費用については米国内で予算措置がまだされておらず，米国向け貨物の積み出しを行っている港は世界中で 600 港以上もあるため，その全てに米国政府のコスト負担で機材を設置することができるとは考え難い．今後，ターミナルオペレーター等が自ら機材を購入しなければならなくなった場合，コンテナをスキャニングする度に利用者から手数料を徴収する可能性があることが指摘されている．

以上のように，完全に実施するにあたっては問題点が多いことは DHS 内部でも認識されている．また，次項で述べる「10＋2」ルールの最終規則案が発表されているが，これを 100％スキャニングの代案とすることを望む声もある．

9）「10＋2」ルール（Importer Security Filing Additional Carrier Requirements）[17)18)]

24 時間ルールで申告される積荷目録情報のスクリーニ

ングだけでは，テロに使用される武器や弾薬の輸入を防ぐには不十分であるとの米国政府の考え方により，24 時間ルールで要求される情報に加え米国内の輸入業者（10 項目）と船社（2 項目）に事前申告を要求する規則である．

2009 年 1 月 26 日から暫定的に施行され，2010 年 1 月 26 日から罰則も含めた完全実施の予定である．この規則に違反した場合罰則規定が設けられており，1 件につき 5,000 ドルの罰金が科せられることになるが，完全実施の 2010 年 1 月 26 日までは罰則なしで運用される．

表-13 に示す通り，輸入業者が申告する事項はサプライチェイン全体に渡る情報である．船社が申告する内容は，貨物輸送経路を追跡する内容である．コンテナ詰め場所については最終寄港地を出帆後，48 時間以内の提出，コンテナステータスメッセージについてはデータ到着後 24 時間以内の提出が求められている．

なお，申請にあたっては，ABI または AMS の電子申告システムを使用することが示されているため，将来的には ACE による申告となることが予測される．

この規則は米国の輸入業者が申告するものであり，輸出者に申告を課せられているわけではないが，米国内の輸入業者が輸出側の荷主等から適切に情報を入手した上で申告を行う必要がある．例えば，輸入業者が米国内で適切な対応を行わない場合，輸出側での輸出が差し止めとなる事態も想定される．

表-13　「10＋2」ルール申告事項

輸入業者の申告データ
◆船積24時間前までに申告必須な事項
① 販売者（所有者）の名前、住所 ② 購入者（所有者）の名前、住所 ③ 記録上の輸入業者番号 ④ 荷受け番号
◆船積24時間前の提出が必須な事項 ただし、米国到着24時間前までに正確な情報に修正可能
⑤ 製造者（サプライヤー）の名前、住所 ⑥ 送り先の名前、住所 ⑦ 原産国 ⑧ 貨物のHTS番号（6桁）
◆米国到着24時間前までにできるだけ早く提出する事項
⑨ コンテナ詰め場所 ⑩ 混載業者の名前、住所
船社の申告データ
① 積み付け計画書 ② コンテナステータスメッセージデータ

3.2 EU における対策と現状 [9)10)17)18)]

EU においては WCO(World Customs Organization：世界税関機構)の WCO SAFE「基準の枠組み」に沿った制度の構築が検討され，2008 年 1 月から AEO 制度が導入されている．AEO 制度とは，保安対策上特定の要件を満たした事業者に優遇措置を与える認定制度である．

EU における AEO 制度導入の目的はサプライチェイン全体での安全確保によってテロや不正を未然に防止することである．よって，AEO の対象者は，輸出入を含むサプライチェインを構成する全ての事業者（製造会社，フォワーダー，運送業者，倉庫業者，通関業者，輸入業者）となっている．

EU における AEO 制度の導入の経緯を**表-14** に示す．

AEO の資格の種類は，(1)税関手続きの簡素化が得られる AEO（タイプ C），(2)セキュリティ・安全性コントロールにおける円滑化が得られる AEO（タイプ S），(1)(2)の両方の優遇を得られるジョイント資格（タイプ F）の 3 種類があり，それぞれの内容については下記の**表-15** の通りである．AEO 資格を取得できる事業者は，EU 内で設立された事業者のうち，「関税法が対象とする活動に関与する者」であり，税関業務に関与しない事業者には申請資格は無い．AEO を取得した場合の利点は**表-15** に示す優遇措置を得られることである．そのためには**表-16** に示す保安管理体制を満たす必要がある．

EU で AEO を付与された企業は 2008 年 9 月 1 日現在で 236 件，受領された申請総数は 1,253 件である．申請手続きに際して，企業は 200 項目の質問を含む 26 頁の申請書に記入しなければならず，また，EU では母国語が多岐にわたることもあり，申請手続きの複雑さから AEO としての認定を避けている企業もある [18)]．

なお，EU 内においては，1 つの EU 加盟国で取得した AEO 資格は，他の加盟国においても同様に認知される．

また EU は他国との相互認証の取組を進めており，今後は EU の AEO 資格を取得すればそれ以外の他国への輸出入の際の優遇措置が受けられる可能性がある．

表-14　EU における AEO 導入の経緯

2003年 7月	セキュリティ問題に関する一連の措置を提案
2005年 5月	「共同体関税規則のセキュリティ上の改正（改正関税法）」公布
2006年12月	「改正関税法施行規則」採択
2008年1月 1日	認可事業者制度（AEO制度）導入
2009年7月 1日	輸出入製品情報の事前申告制度導入予定
2010年	関税法　再改正予定

表-15　AEO の資格内容（EU）[9)10)]

タイプ	(1) 税関手続きの簡素化ベネフィットが得られるAEO	(2) セキュリティ・安全性コントロールにおける円滑化が得られるAEO	(3) 税関手続きの簡素化とセキュリティ・安全性の両方のベネフィットが得られるAEO (ジョイント資格)
対　象	税関のコンプライアンス基準、適切な記録保持基準、財務の健全性の基準を満たす、EU内で設立された事業者	税関のコンプライアンス基準、適切な記録保持基準、財務の健全性の基準、セキュリティ・安全性基準を満たす、EU内で設立された事業者	(1)、(2)の優遇措置の適用を望む事業者
優遇措置	・ 物理検査及び提出書類の軽減 ・ 税関が検査を実施する場合の優先的取扱い ・ 検査の実施場所の選択 など	・ 物理検査及び提出書類の軽減 ・ 税関が検査を実施する場合の優先的取扱い ・ 検査の実施場所の選択 ・ 簡易申告のための提出データの軽減 ・ 事前通告　など	・ 物理検査及び提出書類の軽減 ・ 税関が検査を実施する場合の優先的取扱い ・ 検査の実施場所の選択 ・ 簡易申告のための提出データの軽減 ・ 事前通告　など

表-16　AEO が満たすべき保安管理体制 [9)10)]

- 建物が不法侵入を防止する素材で作られていること
- 出荷エリアや船積みドック、貨物エリアへの不法侵入を防止するための適切なアクセスコントロールが存在すること
- 貨物への不正な変更・改ざんの防止のための適切な措置がとられていること
- 禁止・制限貨物と他の貨物との区別に関する輸出入ライセンスの取扱いで、適切な手続きが行われていること
- 事業者が、国際的なサプライチェインのセキュリティを確保できるよう、取引先を特定するための明確な基準を有していること
- 従業員の選定に際して、セキュリティ上の審査を行い、定期的な経歴検査を実施していること
- 従業員をセキュリティに関する認識向上プログラムに参加させていること

3.3 国際機関等における対策

1）WCO における対策 [8)11)]

WCO は，世界の 99%の税関当局が参加しており，税関制度の調和・統一を推進し，関税行政の国際協力の推進により国際貿易の発展に貢献することを目的に設立された組織であり，国際貿易の安全性確保に関するガイドライン等の作成・推進も行っている．

「WCO では，国際貿易の安全確保と円滑化を両立させるための方策について，米国や日本を含む 12 ヶ国で検討が行われた．その検討結果は，「国際貿易の安全確保及び円滑化のための WCO・SAFE（Security and Facilitation in a Global Environment）「基準の枠組み」としてまとめられ，2005 年 6 月の総会で採択された．その後，2006 年 6 月に AEO の要件や付与できる便益等について解説した「AEO ガイドライン」が採択され，2007 年 6 月の総会で，「基準の枠組み」に「AEO ガイドライン」の内容を包括する改正が行われた．

この「基準の枠組み」は，世界レベルで AEO プログラムを実施するための最低基準となる技術的ガイダンスを規定するものである．AEO 制度は，元々は WCO の枠組みによってできたシステムであり物品管理の効率性を高めるための税関の能力を向上させることで，物品の通関及び引渡の迅速化（優遇措置の付与）が目的である．また，商業の安全確保及び円滑化の観点から，異なる複数の保安対策に関する要求により国際貿易に過度の負担を強いないようにするため，他の政府の要請と重複したり矛盾したりしない国際的な税関の基準となっている．この「基準の枠組み」の目的等については，**図-4** に示す通りであり，4 つの要素と 2 つの柱から構成されている．図中の要素（1）については 24 時間ルール等の事前申告制度，（2）は米国での ATS（Automated Targeting System：ハイリスクコンテナの自動検知システム）に相当するスクリーニング技術，（3）は CSI 等の貨物スキャニング，（4）は AEO 制度に対応した記述であり，セキュリティ対策における実施の柱として定めたものである．この 4 つの要素が必要な理由としては，下記の事項が挙げられる．

①電子媒体による事前貨物情報：時間内に十分なリスク評価を実施するために，貨物及びコンテナの積荷に関する事前電子情報が必要である．

②国際的整合のとれたハイリスクコンテナの選定：電子データを用いた自動検知システムを使用することにより，仕出港やそれ以前のサプライチェインにおけるで

きるだけ早い段階でのハイリスクコンテナの特定に必要である．

③輸出国による非破壊探知機器を使用した貨物検査：貿易の流れを阻害することなしに迅速に検査するために必要である．

④優遇措置の明確化：SAFE「基準の枠組み」の効果的な実施のためには，貿易の安全確保と同時に，貿易の円滑化も考慮しなければならない．そのためには，保安対策に応じた優遇措置を明示し，両者の調和を取るために必要である．

また，現在では各国の AEO 制度の連携が進められており，相互認証に向けた取組がなされている．

しかし，各国の制度はそれぞれ内容が異なっている．例えば，米国の C-TPAT では輸入に関係する事業者のみが対象，EU の AEO 制度では，輸出入に関係する事業者が対象，ニュージーランドの AEO 制度である SES(Secure Export Scheme)では輸出に関係する事業者が対象であり，対象とする事業者が同一でない．よって，実際に相互認証を実現させるには自国と相手国の制度の相違による問題点を明らかにし，お互いに十分信頼できる制度であることを確認した上で取り組んでいかなければならず [11]，今後取組が必要な分野と考えられる．

このような状況の中で，まず，米国とニュージーランドが 2007 年 6 月に相互認証で世界初の合意に至った．現在において相互認証の取組がなされているのは，表-16 の通りであり，多くが協議や研究段階である．わが国については，ニュージーランドの間で，2008 年 5 月 14 日に双方向の相互認証の取り決めに署名し，実際に 10 月 20 日から実施されている [11]．

表-17　相互認証取組の経緯

2007年 6月	米国－ニュージーランド 相互認証で合意 《世界初の試み ただし、ニュージーランドから米国への一方的な物流のみが対象》
2007年11月	米国(C-TPAT)とEU(AEO)について2009年を目標に相互認証に向けて協力開始
2008年 2月	米国－ニュージーランド 相互認証協定に署名
2008年 3月	米国税関・国境警備局(CBP)とEUの税制・関税同盟局 C-TPATとAEOの2009年相互承認実現に向けたロードマップ協定に署名
2008年 5月	日本－ニュージーランド AEO相互認証取決めに署名 《双方向の物流を対象とした取組としては世界初》
2008年 7月	米国税関・国境警備局(CBP)は、 ヨルダン： 「Golden List Program」 カナダ ： 「Partners in Protection Program」 と、サプライチェーン保安制度の相互承認協定を締結 更に、日本・シンガポール・オーストラリア・メキシコと、相互承認を協議中
2008年10月	日本－ニュージーランド 相互認証実施

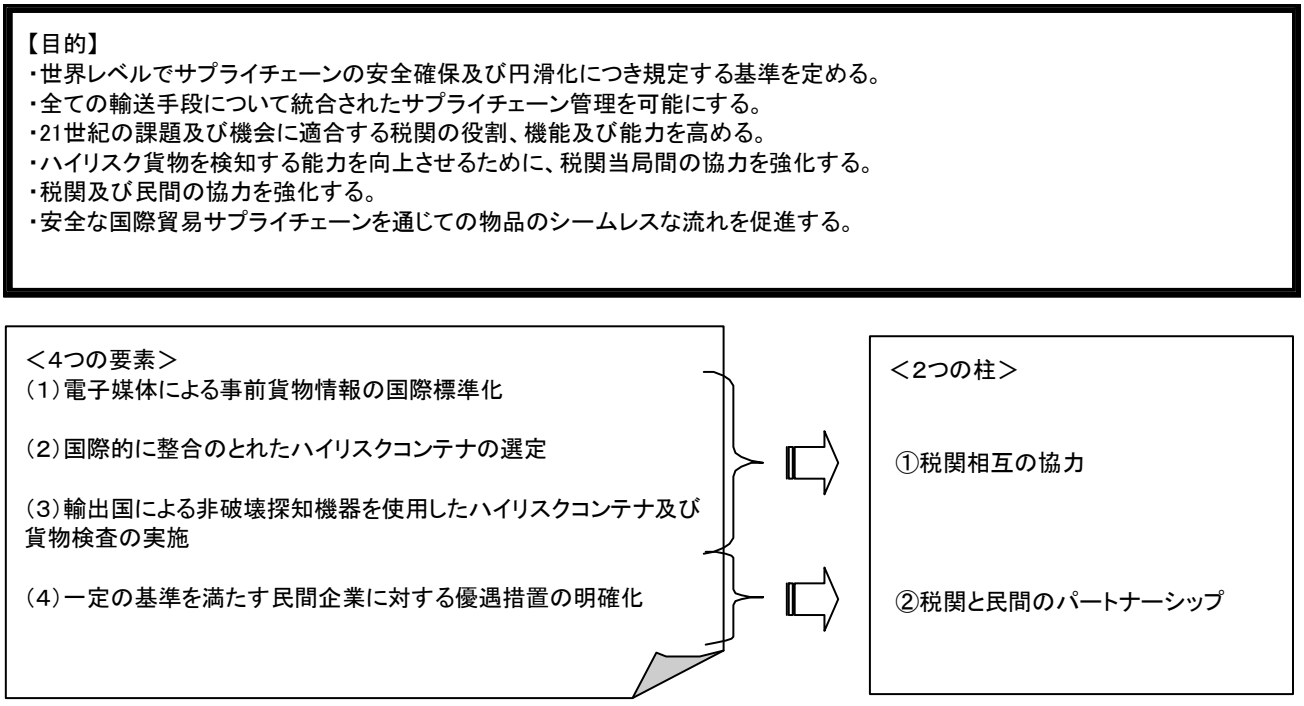

図-4　WCO SAFE「基準の枠組み」目的及び要素

２）ISO における対策 [12)]

ISO28000 シリーズは，国際間の物流セキュリティの国際標準化を目的とし，2007 年に発効したサプライチェインセキュリティ関係の国際規格である．**表-18** に ISO28000 シリーズの概要，**表-19** に ISO28000 の取得要件の例を示す．

現在，ISO28000 シリーズは**表-18** の通り発効され，主に DP World 社等のターミナルオペレーターが取得している他，2008 年 3 月 27 日に，米国ヒューストン港が港湾管理者として世界初の認証を取得した．また，アジアにおいても韓国が，企業の物流保安体制の構築を活性化するために，ISO28000 認証制度を導入すると 2008 年 4 月に発表している [20)]．釜山港の PNC コンテナターミナルが 2008 年 4 月 7 日に IS028000 の認証を取得している．

表-18　ISO28000 シリーズ概要

規　格	名　　称	概　　要	発効年
ISO28000	Specification for security management systems for the supply chain サプライチェインのためのセキュリティマネジメントシステムの仕様	物流監視機能の強化、密輸の撲滅、海賊行為、テロ攻撃の脅威への対処、安全なグローバルサプライチェイン体制の整備が目的。 セキュリティの改善・向上を求めるためのリスクベースのアプローチ方法を規定した包括的なマネジメント規格。	2007年
ISO28001	Security management systemis for the supply chain -Bestpractices for implementing supply chain security, assessments and plans -Requirements and guidance サプライチェインのためのセキュリティマネジメントシステム -サプライチェインセキュリティ実施のための最適実施手順- -評価および計画	武器や危険な密売品の輸出入を予防するため、製品・サービスの出荷から輸送手段を通じてエンドユーザーに届くまでの情報の流れ及び貨物の保安レベルを向上させ、国際的なサプライチェーンのセキュリティを強化することが目的。 サプライチェーンのテロ脅威に対する脆弱性を評価し、適切なセキュリティ計画の作成方法を規定すると共にWCO（世界税関機構）が求める「基準の枠組み」及び認定事業者基準（AEO）の要求への適合を支援する規格。	2007年
ISO28003	Security management systemis for the supply chain -Requirements for bodies providing audit and certification of supply chain securitymanegement systems サプライチェインのためのセキュリティマネジメントシステム -サプライチェインセキュリティマネジメントシステムの審査・認証機関を対象とする要求事項	ISO28000の認証（外部監査［第2者及び第3者認証］）を行う監査機関の要件を定めることが目的。	2007年
ISO28004	Security management systems for the supply chain -Guidelines for the implementation of ISO 28000 サプライチェインのためのセキュリティマネジメントシステム -ISO 28000実施のためのガイドライン	ISO28000の内容を解釈するに当たっての実施指針を定めることが目的。	2007年
ISO28005	Electronic Port Clearance 電子式船舶入出港手続き	船舶入出港に関する電子式情報交換えを定め、シングルウインドウを推進することが目的。 船舶入出港に関する電子式情報、データ送信方法を規定する。	未発行
ISO20858	Ships and marine technoligy -Maritime port facility security assessments and security plan development 船舶及び海洋工学 -海事港湾施設のセキュリティ評価とセキュリティ計画の作成	SOLAS（第ＸＩ-2 章）のISPSコードの内容を解釈するに当たっての実施指針を定めることが目的。 ISPSコードで要求されている海事港湾施設の評価及びセキュリティプランの作成方法を規定するとともに、同施設のセキュリティレベルの改善・向上を図るための規格。	2007年

表-19　ISO28000 の取得要件の例（ISO28001 より）

サプライチェイン保安の管理	・ サプライチェインの保安に対応した管理体制 ・ サプライチェイン保安担当者の存在
保安計画書	・ 上流および下流のビジネスパートナーに対して組織が期待する保安内容が計画書で扱われていうこと ・ 危機管理、ビジネス継続性、保安回復の計画書が備わっていること
資産の保安	・ 建物の物理的セキュリティ ・ 外周部および内周部の監視と管理 ・ 施設、輸送具、積荷場および貨物エリアへの不正アクセスを禁止するアクセスコントロールの実施、並びに身分証およびその他のアクセス要素の発効
要員の保安	・ 保安職務に関し、従業員の完全性を雇用前および定期的に評価する ・ 保安職務の遂行にあたり、従業員の具体的教育訓練を実施
情報セキュリティ	・ 貨物と出荷書類の一致の確認 ・ ビジネスパートナーからの貨物情報が正確かつ遅延なく報告されている ・ 不正アクセスおよび情報の悪用を防止する仕組み
物品と輸送具の保安	・ すべての出荷、積荷場および閉鎖された貨物輸送ユニットの保管場所に対する不正アクセスを制限、検出および報告する手順が備わっている ・ 保安の規則、手順、指針を輸送業者に提供している
閉鎖された貨物輸送ユニット	・ 輸送の途中で輸送具の保護主が変わるときにシールに工作の痕跡がないか点検する

4. 考察

4.1 サプライチェインセキュリティ対策に関する現状の評価

2001 年 9 月の米国同時多発テロ以降，米国や日本などの各国や EU，WCO などの国際機関が，コンテナ貨物のハイジャックやコンテナの不正使用などのテロの脅威への対策として，様々な保安対策を講じてきた．

しかしこれらの対策を講じるには費用や輸送時間の増加が発生するため多額の費用と物流効率化への影響を費やしてまでも対策を講じることが良いのか意見は分かれている．

対策を講じたことによる効果については，肯定的な意見として，対策を講じるようになって以後，コンテナを利用したテロは発生しておらず，これは対策を行っていることが広まったことにより，コンテナを利用したテロが困難となったというものである．

否定的な意見としては，費用に見合った効果が発揮されているか疑問であるという以下のものが挙げられる．

24 時間ルールに関しては，リードタイムの延長による在庫の負担等の費用増加が大きいというものである．

C-TPAT に関しては，日本の企業に関しては，従前より保安対策が十分で税関当局から信頼されていたために，取得による優遇措置をさほど感じられないとの意見もある一方，C-TPAT 取得後，貨物の検査頻度が増加していないため，これが優遇措置であるとの意見もある．また C-TPAT を取得した企業による貨物は，米国の港湾が有事の際においても，優先的に貨物輸送が復旧できることを期待する声もある．

各国において異なった AEO 制度が乱立してきていることにより，諸外国との取引のある企業は C-TPAT を取得しているにも関わらず，別途 EU の AEO を取得しなければ，EU における優遇措置を受けられない等の不便が生じている．これは二国間・多国間において，それぞれの AEO 制度を相互認証によって解決できることであるため，今後相互認証に向けての各国の協力が必要不可欠である．

4.2 サプライチェインセキュリティ対策に関する今後の見通しと課題

今後の世界的なサプライチェインセキュリティ対策の進展する方向としては二つの可能性が想定される．

第一は，サプライチェインの中でも特に水際対策を強化するという考え方である．水際対策とは，米国の 100%スキャニングのように，各国の輸出入時における国境にて危険を阻止しようとする対策のことである．従来以上の物流への影響（輸送費用，輸送時間の増加等）が懸念されるが，サプライチェインには関わる主体が多いため

サプライチェイン全体での保安対策を確保することは容易でないことから，米国政府の関心は依然として高い．

第二は，サプライチェイン全体でのバランスの取れた対策である．これは特定の箇所における対策を強化するよりもむしろ，サプライチェイン全体の各部分において対策を講じようとするものである．具体的には，貨物情報の詳細な分析（ハイリスク貨物の選定）や，IC タグ等を利用した貨物のリアルタイム追跡，サプライチェイン全体に亘る物流施設でのアクセス管理等がある．

ただし例えばICタグの利用ひとつを見ても課題も多く，貨物は世界的なサプライチェイン全体において輸送されることから関係者が多く，タグの読み取り機等のインフラ部分のコスト負担の調整という課題があり，また各国により異なる電波の使用周波数帯の整合性確保の問題をクリアする必要がある．

また，貨物情報のリスク分析についてはまだ十分手法が確立されていない．今後は，各国・各地域の犯罪やテロに関するリスクの状況に応じハイリスクな貨物を確実に特定できるような事前スクリーニングの技術を確立することが必要と考えられる．

4.3 今後の港湾への影響

今後世界の保安対策のうち「水際対策の強化」ないしは「サプライチェイン全体でのバランスのとれた対策」のいずれに進む場合でも，港湾の果たす役割は大きい．

例えば米国の 100%スキャニングが実施されれば，大量のコンテナ貨物が港湾に滞留する可能性があり，物流への影響を最低限となるような工夫が必要となる．貨物のコンテナターミナル内での輸送経路ならびに RPM, OCR, NII 等のスキャニング設備の配置に考慮したターミナル計画手法の開発等が必要となる．

また IC タグ等を利用した，サプライチェイン全体を通じての貨物のリアルタイム追跡を世界のサプライチェインにおいて活用するためには，港湾においてタグの読み取り機等の設備を整備することが不可欠となる．

世界では，既にサプライチェインセキュリティへの積極的な対応が始まっている国もある．

ロッテルダム港では，SFI のパイロットプログラムの結果，100％スキャニングを実施するためには，物流を阻害せずに，貨物を検査できるような港の大規模な改造が必要となる等の様々な問題が発覚したにも関わらず，今後の進展に備え，ゲートでのすべての輸出コンテナのスキャニングを計画し，米国による 100％スキャニングの実施に応じる予定である．このことにより，ロッテルダム港から輸出された貨物の米国での検査率の減少による EU 内での競争力の強化を期待している（「グリーンレーンポート」）．

また，韓国では，ISO28000 の導入をきっかけとして，国内の物流全般にわたって国際水準の輸送保安対策を確保することができると期待されている．

今後は，ISPS コードの遵守という，港湾施設に特化した保安対策だけではなく，国際輸送の安全性にも配慮した港湾が他のサプライチェインメンバーからの信頼を得て，またその港湾を通過する貨物検査率の減少というメリットを得ることにより競争力を強化させる可能性がある．

５．おわりに

本資料では，現在実施ないしは実施が検討されている海外各国・国際機関における海事輸送を中心としたサプライチェインセキュリティ強化の取組状況について取り纏めた．多くの対策において実施上の課題が残されており，今後一層，各国・各機関にて試行を重ね，より効果的な対策を検討していくことが必要である．港湾をはじめとした我が国における国際輸送に関わる主体においても，世界的動向を十分に見極めつつ，適切な対応を図る必要がある．

特に，サプライチェイン全体での保安の確保は，自国のみの対策では不十分であり，他国とも協力体制を整えながら実施していくことが必要不可欠である．

今後は引き続きこのような世界的な国際輸送保安対策の動向の継続的調査を行うとともに，保安対策の強化と物流の効率性の確保の両立が大きな課題となっているため，
これらを両立させるための手法（港湾ターミナルにおける施設配置上の工夫や，情報通信機器の導入，サプライチェイン全体の管理のための物流情報化[13)] 等）に関する事例収集や検討を行う予定である．

（2009 年 2 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) 日本貿易振興機構（ジェトロ）: 米国物流セキュリティ規制に関する調査報告書　2008 年 5 月
3) 日本貿易関係手続き簡易化協会：平成 18 年度 セキュ

リティ強化の環境下における貿易手続き簡易化特別委員会報告書
4) Strategy to Enhance International Supply Chain Security July 2007
5)ボレロ(株)：国際取引の枠組みを根底から変える米国税関新システム(ACE)　bolero update vol.14 2003
6)ボレロ(株):米国の ACE 導入と英国, 豪州の動き　bolero update vol.15 2003
7) U.S. Customs and Border Protection : Report to Congress on Integrated Scanning System Pilots
8) 世界税関機構（WCO）：SAFE「基準の枠組み」
9) 日本貿易振興機構（ジェトロ）:EU の認可事業者（AEO）制度　ユーロトレンド　2008.4
10) デロイト トウシュ トーマツ：EU における国際物流円滑化とサプライチェーン・セキュリティー認定事業者制度(AEO)の導入とその影響－ 国際税務 8 月号 Vol.28
11) 財務省 ファイナンス 2008.7
12) 渡邉豊：国際物流のための ISO28000 入門
13) 宮地豊：「サービスレベルの向上とセキュリティーの確保へ向けた国際港湾物流の情報化について」 北九州港 第 84 号 2004 年 1 月 (社)北九州港振興協会
14) 外務省 HP
15) 財務省 HP
16) 国土交通省 HP
17) 日本機械輸出組合 HP
18) (財)運輸政策研究機構 HP
19) (財)日本税関協会 HP
20) Korea Trade-Investment Promotion Agency HP

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
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
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・スキャニング能力強化プログラム
NII(Non Inteusive Inspection System)：非開封検査装置
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(Radeo 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)：サプライチェイン
SCS(Supply Chain Security)：サプライチェインセキュリティ
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. 528 March 2009

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