日本財団 助成事業
The Nippon Foundation

標準化ニュース No.3

# 海事セキュリティに関する状況報告書

2007年3月

財団法人日本船舶技術研究協会

# 目　次


| 表　　題 | 頁 |
|---|---|
| はじめに | 1 |
| 1.　ISO 28000 シリーズ（サプライチェーンセキュリティ関係国際規格）の概要 | 2 |
| 2.　ISO 28000 シリーズへの国内対応 | 7 |
| 2.1　これまでの対応 | 7 |
| 2.2　今後の対応 | 9 |
| 3.　米国でのサプライチェーンセキュリティ情勢の最新情報 | 10 |

# はじめに

当協会では、日本財団の助成事業として、これまで海事セキュリティに関する調査・研究を行い、国際海事機関（IMO）、国際標準化機構（ISO）などの規則・基準の策定に積極的に関わっています。

米国における 9・11 以降、海事分野においても各方面で保安対策が進められており、IMO においては、2004 年 7 月 1 日に SOLAS 条約第 XI-2 章及び ISPS コード（船舶及び港湾施設の保安のための国際コード）が発効し新たな保安制度が導入されましたが、既にこの条約の実施に係る各種問題点が指摘されており今後問題点を調査し必要な修正を行うことが検討されています。

また、海事保安をめぐる国際的な動きは IMO に限らず広くダイナミックに展開しており、米国では C-TPAT、バイオテロリズム法等独自の海事保安強化を図っているほか、世界税関機構（WCO）でも国際サプライチェーン・セキュリティ及び貿易円滑化のためのスタンダードを策定しつつあります。

さらに、ISO においてもコンテナ物流の急増を背景として国際的なサプライチェーンのセキュリティを確保する観点から一連の保安管理システム規格が審議中であり 2007 年には順次発行する見込みです。

このうち、ISO/TC 8（船舶及び海洋技術専門委員会）での海事セキュリティに関する審議については、当協会が国内代表窓口を務めており、日本財団助成に基づく当協会／船舶関係工業標準化事業として、当協会／標準部会の下に TC 8 セキュリティ分科会を設置し、最適な ISO 規格の構築に積極的に取り組んでいます。

ISO/TC 8 で取り扱っている海事セキュリティ ISO 規格（ISO 28000 シリーズ）は、船舶分野（海上輸送）のみならず、生産又はサプライチェーンの全てをも含む物流全体のテロ対策の一環として、上記に係る企業、団体等の保安レベルの向上に資することを目的とした保安関係国際規格の体系であり、今後サプライチェーンに関与する多くの事業者に大きな影響を与えることも予想されます。

そこで、本報告書では ISO/TC 8 に於ける海事セキュリティに関する国際規格案の概要、審議状況、国内取り組みをご報告させて頂くと共にセキュリティの最先端を行く、米国でのサプライチェーンセキュリティ情勢の最新情報についてご報告させて頂きます。

## 1. ISO 28000 シリーズ（サプライチェーンセキュリティ関係国際規格）の概要

本シリーズは、2001 年 9 月 11 日の同時多発テロ以降、米国を中心に作成が進められており、船舶分野（海上輸送）のみならず、生産又はサプライチェーン*1 の全てをも含む物流全体のテロ対策の一環として、上記に係る企業、団体等の保安レベルの向上に資することを目的とした保安関係国際規格の体系であり、今後サプライチェーンに関与する多くの事業者に大きな影響を与えることも予想されます。

> *1 サプライチェーン（supply chain）：
>
> 資源、材料の調達に始まり、製品・サービスの出荷を経て輸送手段（陸上・海上を含む）を通じてエンドユーザーにまで及ぶプロセス。

ISO/TC 8（国際標準化機構／船舶及び海洋技術専門委員会）は、当初、SOLAS（第 XI-2 章）の ISPS コード（船舶及び港湾施設の保安のための国際コード－2004 年 7 月 1 日発効済）の発効に合わせて、ISO/PAS*2 20858（海事港湾施設の保安評価と保安計画の開発）を開発・制定しました。

> *2 PAS: Publicly Available Specification：
>
> 国際規格（ISO）の制定の手順に先立って発行される中間仕様書。迅速な開発や発行が優先する場合に用いられ、制定した時点で、プロセスを進めて ISO 規格とすべきかを速やかに決定します。

さらに、サプライチェーン全体の保安レベル向上の方策をより具体化するために、2005 年初頭から、28000 シリーズの整備・策定に着手し、現在次のとおりの規格が公開仕様書（PAS）として発行され、且つ ISO 規格制定に向けた審議の最終段階にあります。

これらの PAS を含む ISO 規格は強制基準ではなく任意でありますが、国によりましては国内法規への導入なども考えられるため、注意を要します。

1) **ISO 28000 － サプライチェーンのためのセキュリティマネジメントシステムの仕様**

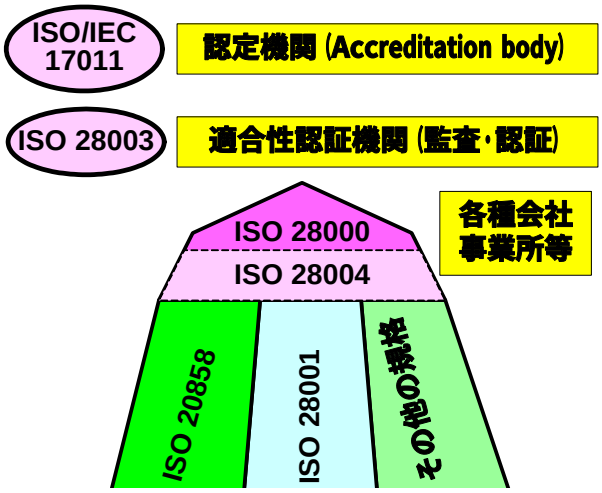
PAS 発行日：2005-11-15

ISO 規格発行見込み：2007 年中旬

2) **ISO 28001 － サプライチェーンのためのセキュリティマネジメントシステムーサプライチェーンセキュリティ実施のための優良実施要領ー評価及び計画**

PAS 発行日：2006-09-01

ISO 規格発行見込み：2007 年下旬




ISO 28000 シリーズの相関関係図

3) ISO 28003 – サプライチェーンのためのセキュリティマネジメントシステムーサプライチェーンセキュリティマネジメントシステムの監査及び認証を提供する機関の要求事項

PAS 発行日：2006-10-05

ISO 規格発行見込み：2007 年下旬

4) ISO 28004 – サプライチェーンのためのセキュリティマネジメントシステムーISO/PAS 28000 の実施のための指針

PAS 発行日：2006-09-01

ISO 規格発行見込み：2007 年中旬

以下、これら ISO 28000 シリーズの概要を紹介します。

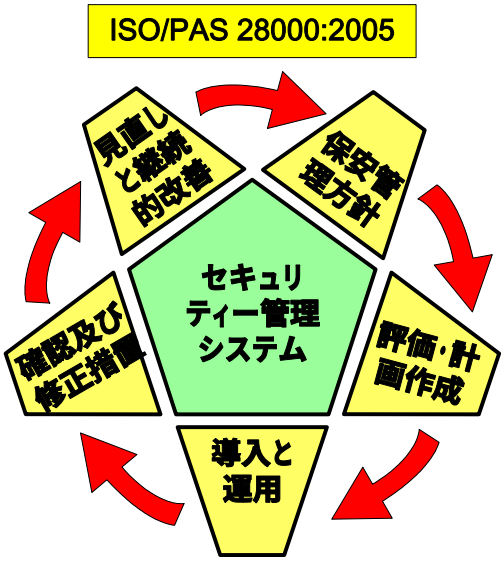
**① ISO 28000　Specification for security management systems for the supply chain**

ISO 28000 策定の目的及び必要性（Purpose and justification）は以下の通りです。

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、そして安全なグルーバルサプライチェーン体制の整備を目的としています。

この規格は、ISO 14000（環境マネジメントシステム）をベースに作成され、PDCA（Plan - Do - Check - Act）サイクルによる継続的な管理システムの向上を規定するもので、2005 年 11 月に PAS として発行され、現在 ISO 規格発行に向けた最終段階の審議が行なわれています。

この規格の構成は ISO 14001（環境マネジメントシステムー要求事項及び利用の手引）をモデルとして、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となっています。



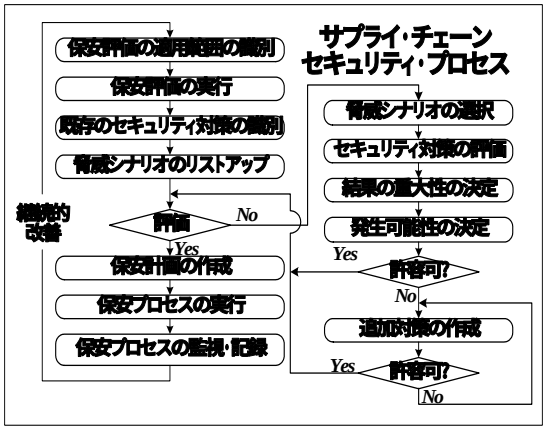

ISO 28000 の PDCA サイクル

**② ISO 28001　Security management systems for the supply chain - Best practices for implementing supply chain security - Assessments and plans**

ISO 28001 策定の目的及び必要性（Purpose and justification）は以下の通りです。

武器や危険な密売品の輸出入を予防するため、この規格では、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強化を目的としています。

この規格は、サプライチェーンのテロ脅威に対する脆弱




サプライチェーン保安のプロセス

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米国の C-TPAT、WCO（世界税関機構）の AEO 基準（認定事業者基準）等の相互承認を進めるに当たっての統一解釈として国際的な期待が寄せられており、ISO 28000 シリーズの中でも最重要案件とされています。

**③ ISO 28003　Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems**

ISO 28003 策定の目的及び必要性（Purpose and justification）は以下の通りです。

上述の ISO/PAS 28000 の認証（外部監査[第 2 者及び第 3 者認証]）を行なう監査機関の要件を定めることを目的としています。

この規格は、ISO/PAS 28000 への適合について判定する第三者機関が満たすべき要件を規定するもので、ISO/PAS 28000 の自己監査（内部監査[第 1 者認証]）（self audit）を行う際には不要とされています。

この規格の構成は、ISO 19011（品質及び／又は環境マネジメントシステム監査のための指針）及び ISO 17021（適合性評価－マネジメントシステムの審査及び認証を提供する機関に対する要求事項）に準拠しています。

**④ ISO 28004　Security management systems for the supply chain -- Guidelines for the implementation of ISO/PAS 28000**

ISO 28004 策定の目的及び必要性（Purpose and justification）は以下の通りです。

上述の ISO/PAS 28000 の策定を受けて、同 PAS 内容を解釈するに当たっての実施指針を定めることを目的としています。

この規格は、ISO/PAS 28000 の節（項目）毎に、意図（Intent）、典型的な入力（Typical input）、手順（Process）、典型的な出力（Typical output）を具体的に規定し、ISO/PAS 28000 適用のためのガイドラインとなっています。

**ドバイ・ポーツ・ワールドは 2006 年 9 月に ISO/PAS 28000 に準拠した認証を LRQA（ロイド・レジスター・クォリティ・アシュアランス）から受けました。**

**また、米国のスターバックスコーヒー社はサプライチェーンのセキュリティを改善するため ISO/PAS 28001 を採用しています。**

以上の 4 規格（ISO 28000、ISO 28001、ISO 28003、ISO 28004）により ISO 28000 シリーズは構成されておりますが、場合により次の 2 規格も含まれることがあります。

**① ISO 20858　Ships and marine technology -- Maritime port facility security assessments and security plan development（海事港湾施設の保安評価と保安計画の開発）**

PAS 発行日：2004-07-01

ISO 規格発行見込み：2007 年下旬（ISO 28001 との整合を行ない審議再開）

ISO 20858 策定の目的及び必要性（Purpose and justification）は以下の通りです。

SOLAS（第 XI-2 章）の ISPS コードの発効を受けて、同内容を解釈するに当たっての実施指針を定めることを目的としています。

この規格は、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例示するとともに、合わせて同施設のセキュリティレベルの改善・向上を図るための指針を定めています。

**② ISO 28005　Ships and marine technology -- Computer applications -- Electronic port clearance（電子式ポートクリアランス）**

PAS 発行日・ISO 規格発行見込み：　未定

ISO 28005 策定の目的及び必要性（Purpose and justification）は以下の通りです。

船舶出入港に関する電子式情報交換、データ送信方法を定め、「単一窓口方式（one stop shopping）」及び／又は「単一窓口（single window）」*3 を推進することを目的としています。

*3 「単一窓口方式（one stop shopping）」及び／又は「単一窓口（single window）」：

1 回の入力・送信で船舶出入港に関する必要な港湾関連手続きを行なうことが出来ること。「シングルウィンドウ」とも呼ばれる。

ヨーロッパの MarNIS プロジェクトに基づく XML*4 技術を利用した、電子式情報交換、データ送信方法をベースとしており、同種の国際基準・国際規格である UN/ECE（国連欧州経済委員会）が開発中の EDIFACT*5 メッセージ、ISO/TC 154（行政・商業・工業用書式及び記載項目専門委員会）が UN とリエゾンを結び開発した ISO/TS 15000 シリーズ（ebXML*6）との整合を図るべく、また、IMO/FAL、各国港湾が使用している XML 技術、セーフ・シー・ネット（EC 指令）等への考慮を行ないながら規格作成を進めています。

*4 XML: Extensible Markup Language：

文書やデータの意味や構造を記述するためのマークアップ言語の一つ。マークアップ言語とは、「タグ」と呼ばれる特定の文字列で地の文に構造を埋め込んでいく言語のこと。

*5 UN/EDIFACT：

現在貿易手続をはじめとしてビジネス全般に亘って幅広く使用されている国連（UN）の管理する電子データ交換（EDI）のための汎用国際基準のこと。

*6 ebXML：

**電子ビジネス拡張可能マーク付き言語のこと。**UN **とリエゾンを結び開発。**

## 2. ISO 28000 シリーズへの国内対応

### 2.1 これまでの対応

これらの ISO 28000 シリーズへの国内対応につきましては、当協会内に TC 8 セキュリティ分科会を設置し、次の原則のもと、国際会議に積極的に日本代表を派遣し、原案作成に積極的に貢献してきております。

**日本としてはセキュリティの重要性は認識するが**

**「第三者認証を伴わない規格作成」を要求する**

サプライチェーンに関わる皆様にこの規格の存在を把握頂くため、また、現在 ISO 28000 シリーズの審議が山場を迎えており、この機会を捉え、ISO 28000 シリーズは何か、サプライチェーン・セキュリティがどう変わるのか、関係当事者にどういった影響を与えるのか、など「海事分野におけるセキュリティ対策の問題点と今後進むべき方向について」をテーマとして、海事セキュリティの専門家（下記）にお集まりいただき、昨年 12 月 20 日に「海事セキュリティに関する専門家による座談会」を開催致しました。

その模様は 2007 年 2 月 7～9 日発行の海事プレス誌に紹介頂くと共に物流情報誌 月刊 CARGO2 月号（海事プレス社）に掲載頂きました。

なお、本会ホームページ（http://www.jstra.jp/html/standard/iso_kotake_0209.html）にもその内容を掲載しております。

**座談会出席者**

【 専門家 】

**橋本　弘二　氏（日本機械輸出組合　部会・貿易業務グループリーダー）**

WCO（世界税関機構）民間協議グループ（PSCG）日本エキスパートとして、主として WCO の策定する「国際貿易の安全確保と円滑化のための基準の枠組み」に係る AEO（Authorized Economic Operator）の審議

当協会　TC 8 セキュリティ分科会委員

**中村　光男　氏（神戸市みなと総局振興部 主幹　ポートセールス担当課長）**

神戸港の船舶・貨物誘致を担当

**樋口　久也　氏（日本郵船株式会社 安全環境グループ 危機管理チーム チーム長）**

船舶保安・サプライチェーンマネジメントセキュリティ関連業務担当

**太田　　進　氏（独立行政法人海上技術安全研究所 運航・システム部門 上席研究員）**

ISO/TC 8/WG 2（セキュリティマネジメントシステム作業委員会）及び ISO/TC 8/SC 11（複合輸送及び短距離海上輸送）/WG 2（サプライチェーンセキュリティのベストプラクティス作業委員会）日本エキスパートとして ISO 28000 シリーズの開発にあたる

当協会　TC 8 セキュリティ分科会委員

当協会　海事保安に係る基準に関する調査研究プロジェクト（SPS）マネージャー

**渡邉　　豊　氏（東京海洋大学 海洋工学部 流通情報工学科 教授）**

ISO/TC 8/WG 2（セキュリティマネジメントシステム作業委員会）及び ISO/TC 8/SC 11（複合輸送及び短距離海上輸送）/WG 2（サプライチェーンセキュリティのベストプラクティス作業委員会）日本エキスパートとして ISO 28000 シリーズの開発にあたる

当協会　TC 8 セキュリティ分科会委員

コンテナ輸送及び港湾実務に関する研究の日本の第一人者

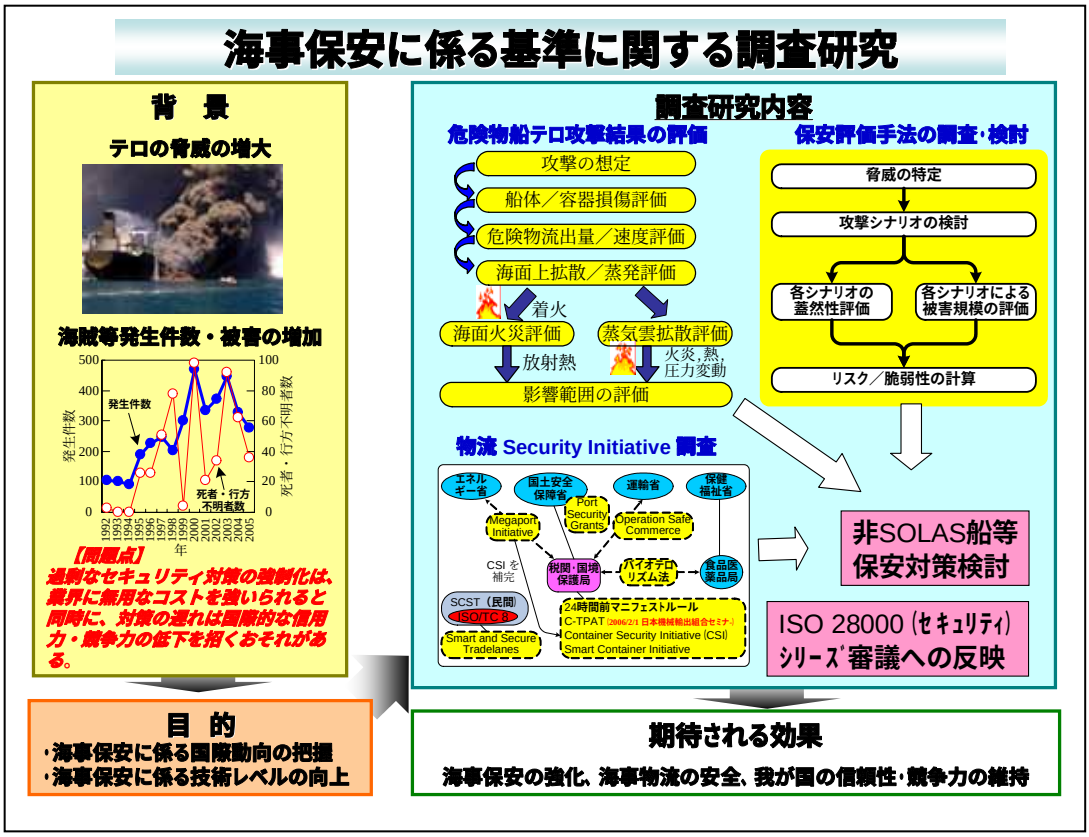
**【 司会 】**

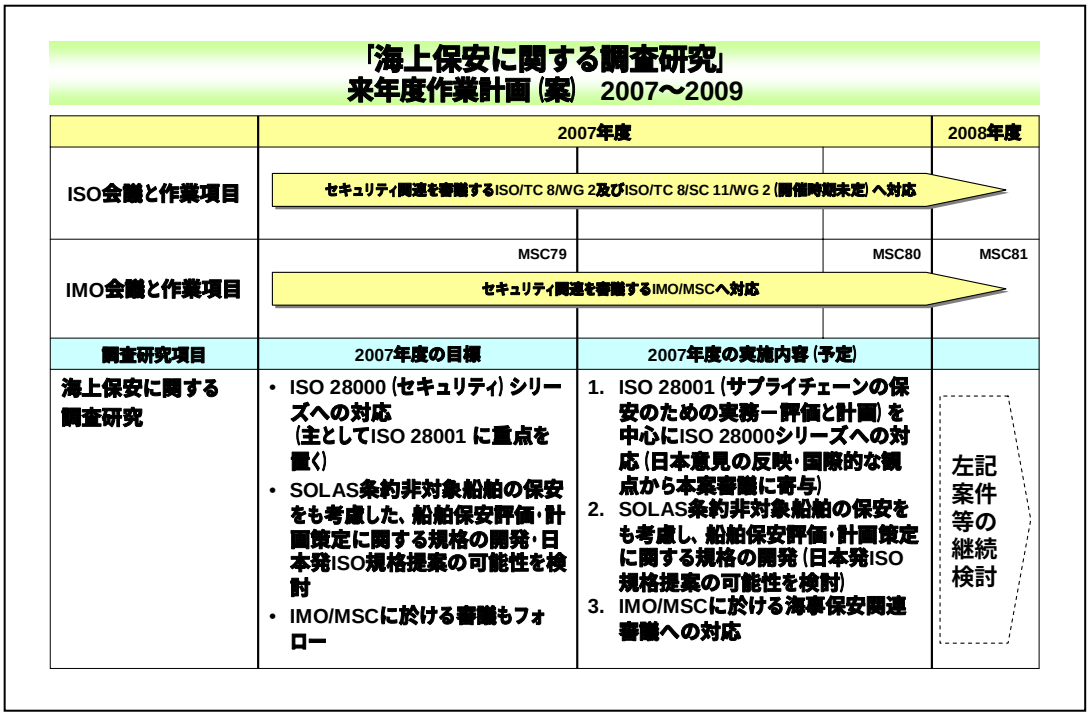
**矢萩　強志　氏（財団法人日本船舶技術研究協会 常務理事）**

これからも最新情報を当協会ホームページ（http://www.jstra.jp/）への掲載及びホットメールでの配信を予定しています。

## 2.2　今後の対応

当協会では本件対応を ISO 対応における最重要案件の一つに位置付け、次のとおりの調査研究の実施を 2007 年度に予定しており、今後も積極的に本件審議に関与する予定としています。



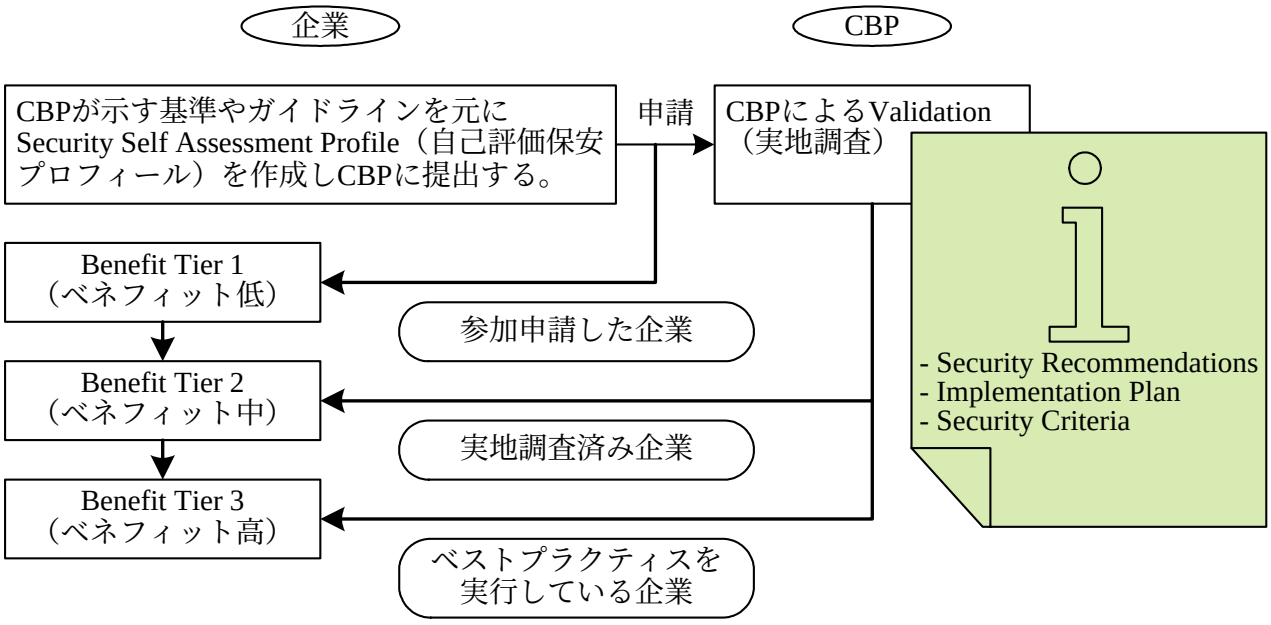
## 3. 米国でのサプライチェーンセキュリティ情勢の最新情報

米国では数年前から電子シールや内部センサーを装備したスマートコンテナ開発に着手しており、今夏にスマートコンテナの仕様を公開する情報があります。

この結果、C-TPAT*[7] TierIIIではスマートコンテナの義務化がされる流れがあります。

*7 C-TPAT：Customs Trade Partnership Against Terrorism

テロリストによる攻撃を抑止及び阻止し、国境の安全を確保し、かつ適正な貿易の円滑化を図るために開発された、官民協同のボランタリー・パートナーシップのこと。現在は CBP が実行している。C-TPAT は 2001 年 11 月に開始されて以来、対象業者を拡大し、戦略計画および保安勧告を作成し、ベネフィットを階層化するなど、発展を遂げてきています。




**C-TPAT 手順の流れ**

C-TPAT 用の Best Practices Catalog が出されておりますが、日本が抱く懸念と同様に「点」でのセキュリティ管理は可能ですが「サプライチェーン」でのセキュリティ維持は難しい旨が読み取れます。

米国が掲げるセキュリティ戦略のうち、荷主が関係するのは次の 3 点です。

① 24 時間ルール

② コンテナセキュリティイニシアチブ

③ C-TPAT

24 時間ルールについては、外国港での船積み 24 時間前までに所定のマニフェストで通知しなければならず、当然ながら、これらを対応しなければならない船会社、輸出者の負担が増大しています。

この関係で更に SAFE Port Act（Security and Accountability For Every Port Act of 2006）が策定されています（米国議会通過：2006.09.30。大統領署名：2006.10.03）。

米国国内輸入者にも 24 時間ルールのタイムリミットに合わせて、海外製造者名、コンテナ詰め場所等の非マニュフェストデータ提出を課す内容が新たに追加されましたが、輸出側荷主への影響は現段階では殆ど無いと思われます。

上記の他、コンテナセキュリティの基準を定め、セキュリティ上で一番の問題である空コンテナのリスク評価のパイロットプロジェクトが 1 年間実施される予定となっております。

テロ対策の一環として、放射性物質検知装置を使用したパイロットプロジェクトを数港で行なう計画であり、次の港での実施を予定しています・

【第 1 グループ】

英国（Southampton）、オマーン（Qasim）、ホンデュラス（Puerto Cortes）

【第 2 グループ】

韓国（Busan）、オマーン（Salalah）、シンガポール（Singapore）

貨物検査に対する SAFE Port Act の定義では、スクリーニング、スキャニング、サーチと 3 種類があり、関係者間では 100%開梱を要求されるのではとの不安・懸念がある模様ですが、行なわれるのはスクリーニング（書面審査）の 100%実施だけであり、この中でハイリスクと判断されたコンテナのみサーチ（開梱）されることになります。

更に、現在米国下院で通っている法案は「HR1」と呼ばれ、外国積出港で 100%のスキャニング実施（放射能・生物化学兵器の検査実施）を求める内容となっています。生物化学兵器をチェックできる技術は現在無く、EU からクレームが付き、議論が行なわれているところです。

これら SAFE Port Act の最新の情報を次頁以降に掲載致します。

（次頁以降の資料は日本機械組合様からご提供頂いたものです）

# SAFE Port Act

**日本機械輸出組合**
**部会･貿易業務グループ 橋本　弘二**
2006年12月19日



## 名 称 と 経 緯

### ➢正式名称

**S**ecurity and **A**ccountability **F**or **E**very Port Act of 2006

⇩

**SAFE** Port Act

### ➢成立までの経緯

- **議会通過**　：2006年9月30日（H.R.　4954）
- **大統領署名**：2006年10月13日
- SAFE Port Act**全文は以下に掲載**

http://www.jmcti.org/C-TPAT/vol.1/2006/C-TPAT_CSI_1-102.htm

# 概　要

- 法文には曖昧な記述が多い反面、多くの条項で短期の期限を定めている。
- 内容通りであれば、2007年中に矢継ぎ早に各種実施規則が発表される。
- 議会の監視が強まっている。
- これまで実施されてきたC-TPAT、24時間ルール、CSIをベースに、貨物検査についてさらに強化される。



# 構　成

- タイトルⅠ　Security of United States Seaports
- タイトルⅡ　Security of The International Supply Chain
  - ✓ Subtitle A – General Provision
  - ✓ Subtitle B – Customs – Trade Partnership Against Terrorism
  - ✓ Subtitle C – Miscellaneous Provisions
- タイトルⅢ　Administration
- タイトルⅣ　Agency Resource and Oversight
- タイトルⅤ　Domestic Nuclear Detection Office
- タイトルⅥ　Commercial Mobile Service Alerts
- タイトルⅦ　Other Matters
- タイトルⅧ　Unlawful Internet Gambling Enforcement

※セキュリティと無関係

## DHSの議会への報告義務
## §201

国土安全保障省（DHS）は、§201で規定されている戦略プランの実施状況を、下記議会委員会に報告しなければならない。

**上院**
①歳出委員会
②商業委員会
③財政委員会
④ホームランド・セキュリティ委員会
- その他　適切な委員会

**下院**
①歳出委員会
②ホームランドセキュリティ委員会
③輸送・インフラストラクチャー委員会
④歳入委員会

**報告期限**
- SAFE Port Act成立後270日以内
- 3年以内に、戦略プランのアップデート

**戦略プラン策定は、議会からDHSへの要請**
- 策定が義務付けられているもの
- 義務ではないが推奨されているもの



## Security of International Supply Chain
## §201　戦略プラン

**義務**
① 国際サプライチェーンにおけるコンテナセキュリティに係る種々の政府および民間セクター参加者その役割と責任
② 不必要な重複や不足の確定と対応措置
③ 関係主体間のコーディネーション向上と国際サプライチェーン・セキュリティ確保のための法令・規則・組織の改変に対する勧告
④ 商業活動（原産地を起点）のセキュリティをさらに確保するため、目的・メカニズム・スケジュール等測定可能なゴールを設定。
⑤ コスト/ベネフィットの評価
⑥ 貨物セキュリティ確保を目的としたボランタリー措置のためのインセンティブ
⑦ 中小企業への影響
⑧ セキュリティの取組み強化のため、民間参加者との情報共有プロセス
⑨ 輸送に係る事件発生時での慎重で“冷静な対応”のための枠組み
⑩ 事件発生の場合の国際貿易の迅速な再開のためのプロトコル
⑪ サプライチェーンセキュリティと他のセキュリティプログラム（旅行セキュリティ、テロリズム金融など）とリンク
⑫ 現行の戦略／プランの調和（National Response Plan National Maritime Transportation Security Plan等々）

**推奨**
- 上の戦略プランを促進するため、コンテナセキュリティのためのベスト・プラクティスを確立するため、外国政府や国際機関によって提案・確立されたセキュリティ・スタンダード、プラクティスを考慮する。

# §203 Automated Targeting System

- マニフェスト･データに加えて追加的なデータを、外国港での積込24時間前までに提出する（現行24時間ルールのタイムリミット） ⇒ 次項
- COACを含めステークホルダーと協議を行なう
- 追加データの提出要求に係るコスト、ベネフィット、フィージビリティ分析を行なう
- 本条項のための実施規則の策定
- ATSのシステムの改善と向上



# §203 10＋2
（11月7日付け Strawman、CBP）

**現行マニフェスト･データ**
Bill of Lading Number
Foreign Port prior to Depart to U.S.
Carrier SCAC
Carrier Assigned Voyage Number
Date of Arrival at First U.S. Port
U.S. Port of Unlading
Quantity
Unit Measure of Quantity
First Foreign Place of Receipt
Commodity Description (HTS/6)
Commodity Weight
Shipper Name
Shipper Address
Consignee Name
Consignee Address
Vessel Name
Vessel Country
Vessel Number
Foreign Port of Lading
Hazmat Code
Container Numbers
Seal Numbers
Date of Departure from Foreign Port
Time of Departure from Foreign Port

**セキュリティ目的追加データ**
**輸入者**
（外国港積込24時間前）
Manufacturer/Shipper name/address
Seller name/address
Container Stuffing Location
Buyer name/address
Ship to name/address
Importer of Record Number
Consignee Number
Country of Origin
Commodity HTS-6

**船社**
Stow Plan
（外国の最後の寄港地出発後48時間）
Container Status Message

**引取り申告データ**
Entry Number/Type
Entry – Port/Entry
Filer Code
Importer of Record
Ultimate Consignee
Surety Number
Filing Date & Time
Importing Carrier
Vessel Name
Country of Origin
Exporting Country
Exporting Date
Foreign Port Arrival
Estimated Arrival Date
Entry Value
HSUSA (10)

Manufacturer ID

## Container Security

### §204 コンテナセキュリティ・基準

- ✓ コンテナセキュリティ・基準を確立する。
- ✓ SAFE Port Act成立90日以内に、策定に着手し、180日以内に暫定規則（Interim Rule)を発表し、2年以内に全てのコンテナが同基準を満たすこと。
- ✓ 空コンのリスク評価のためのパイロット・テストを1年間実施しなければならない（§235）。

### §205 CSI

- ✓ CSIに法的根拠を付与する。外国港のCSI参加を指定する際の要素を明確にする。
- ✓ 議会による監督が強まる。
- ✓ 海外港での検査要件－非破壊検査装置・放射性物質検知装置の使用に係るMinimum Technical Capability、Standard Operating Procedureの確立



## C－TPAT（1）

### §211

- ✓ 政府と民間とのボランタリー・パートナーシップに法的根拠を付与。

### §214ー216

**Tier 1ベネフィット**：認定（Certified）を受けた参加者：ATSスコアリングでハイリスクと判定されるポイントの20%を上回らない。
法成立後180日以内にC-TPAT参加認定ガイドラインを策定。

**Tier 2ベネフィット**：実地調査（Validation）を受けた参加者。Tier1参加者と同じATSスコアリング＋低い検査率の適用＋コンプライアンス理由で検査される場合の優先取り扱い
法成立後Tier2のためのValidationガイドライン策定。

**Tier 3ベネフィット**：ベスト・プラクティスを実施している参加者。迅速な貨物リリース＋いかなる検査目的でも優先的取り扱い＋さらに低い検査率＋さらに有利なATSスコアリング
法成立後2年以内にTier3のためのValidationガイドライン策定

# C－TPAT（2）

**§217**

- C-TPAT参加資格の剥奪・中断手続の策定。
- 民間からの不服申し立て手続の策定。

**§218**

- 第三者機関によるValidation実施のための1年間のパイロット・テスト計画。
  （中国でのValidation及び米国検査官に生命の危険が及ぶと予想される国へのValidationに第三者機関を利用する）

**§219**

- 再バリデーションのフレームワーク構築。少なくとも4年に一度再バリデーションを受けるべき企業を確定するためのフレームワークを構築する



# §231 Pilot Integrated Scanning System

- 非接触型イメージング機器と放射性物質検知装置を組み合わせた統合型スキャニング・システムのパイロットテストのための外国の3港を法成立後90日以内に指定する。
- 法成立後1年以内に当該3港で、統合スキャニング・システムのパイロット・テストをフル・スケールで実施しなければならない。
- フル・スケールの実施とは以下を含む：
  （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

Secure Freight Initiative

2006年12月7日発表

パイロット・テストを行なう3港（第1グループ）

- ✓ 英国：Southampton（2007年6-7月）
- ✓ オマーン：Qasim(2007年2月)
- ✓ ホンデュラス：Puerto Cortes(2007年2月)

第2グループ3港

2007年末までには稼動予定

韓国：Busan

オマーン：Salalah

シンガポール：Singapore

## §232　100%　Screening・Scanning

(1) 外国発のコンテナについて、“ハイリスク・コンテナ”発見のため100%スクリーニングを実施する。
(2) 上記により“ハイリスク”と確認されたコンテナに対して100%スキャニングと開扉検査を実施する。
(条文に明らかな誤りがあるため、スキャニング実施が米国到着前か外国港出発前か不明)

- ✓ (1) については期限が定められていない。
- ✓ (2) については、“as soon as possible”とされている。

## §236　情報共有と官民協力

- ✓ サプライチェーンのリスク情報の収集と共有のためのシステムを開発しなければならない。

## §405　ITDS (International Trade Data System)

- ✓ 輸入および輸出に係るクリアリングあるいは許認可手続きのために書類を要求している官庁は、全てITDSに参加しなければならない (must)
- ✓ 積降港から最終仕向け地までの保税輸送貨物に対するトラッキングを強化する措置を検討すること。

**お問い合わせ：**

〒105-0003

東京都港区西新橋 1-7-2　虎ノ門高木ビル 5 階

財団法人　日本船舶技術研究協会

基準･規格グループ／標準化チーム

TEL 03-3502-2130　FAX 03-3504-2350

Email: info@jstra.jp　URL: http://www.jstra.jp/


この事業は競艇の交付金による日本財団の助成金を受けて実施します。