

# サプライチェーン セキュリティ規格

*ISO 28000 シリーズ*

# SC セキュリティマネージメント規格

1. セキュリティ規格策定の背景

2. ISOにおけるセキュリティ関連規格

3. ISO/PAS 28000シリーズ

4. ISO/PAS 28000 & 28004

5. ISO/PAS 28001

6. ISO/PAS 28003

7. セキュリティに関する国際動向

# 1. セキュリティ規格策定の背景

## 国際海事機関 (IMO) の動向

### 海賊等不法行為に対する対策

例えば、1985年11月20日 第14回総会決議594号  
船舶の乗員・乗客の安全および保安を脅かす不法行為対策

### 2001年9月11日 米国同時多発テロ事件

- 2002年12月12日 海上人命安全条約改正 (新XI-2章)  
&国際船舶・港湾施設保安規則  
(ISPS Code) **採択**
- 2004年 7月 1日 海上人命安全条約改正第XI-2章  
&国際船舶・港湾施設保安規則  
(ISPS Code) **発効**

# 1. セキュリティ規格策定の背景

## ISPS Codeの概要

- (1) 保安責任者の決定
- (2) 保安の評価
- (3) 保安計画の策定
- (4) 保安計画の実施
- (5) 保安の再評価および保安計画の継続的改善
- (6) 保安関係装置の設置  
(保安警報装置、長距離船舶識別・追尾装置)

# 1. セキュリティ規格策定の背景

## ISPS Codeの適用範囲

### 海上人命安全条約 (SOLAS条約) 適用対象船舶

- 国際航海に従事する総トン数500トン以上の貨物船
- 国際航海に従事する旅客船

SOLAS条約適用対象船舶が出入りする港のうち、船舶とのインターフェイス部分 (港湾施設)

適用対象外の船舶、港湾施設があり、  
港湾では、水際しか規則が適用されない

# 1. セキュリティ規格策定の背景

ISPS Codeの補完のため、米国はISO/TC8に、  
港湾の保安規格の策定を提案

- 2004年7月 ISO/PAS 20858  
海事港湾施設の保安評価と保安計画の開発
- 目的: 大量破壊兵器が**米国**に入ること

兵器の密輸防止のためには、物流全体で保安対策を  
実施することが期待される

物流全体を網羅するには、運送事業者のみならず、  
物流に関与する多くの事業者(製造業)の関与が必要

- サプライチェーンセキュリティ規格の提案

## 2. ISOにおけるセキュリティ関連規格

ISO/IEC JTC1 SC26

情報技術のセキュリティ対策

ISO TC34

食品セキュリティマネジメント

ISO TC68

銀行および金融業のセキュリティマネジメント

ISO TC8 (船舶および海洋技術)

サプライチェーンセキュリティマネジメント

## 2. ISOにおけるセキュリティ関連規格

### 全体調整

ISO/技術協議委員会 (Technical Management Board)  
セキュリティアドバイザリーグループ

ISO/PAS 28000が、サプライチェーン以外の  
セキュリティマネージメント (保安管理) の規格として  
使えるかどうか検討中



### 3. ISO/PAS 28000シリーズ

#### (1) ISO/PAS 28000:2005

- サプライチェーンのための保安管理システムの仕様

#### (2) ISO/PAS 28001

- サプライチェーンの保安のための実務
- 評価と計画

#### (3) ISO/PAS 28004

- サプライチェーンのための保安管理システム
- ISO/PAS 28000:2005の実施指針

#### (4) ISO/PAS 28003

- 保安管理システム
- サプライチェーン保安管理システムの監査と承認を実施する機関の要件

### 3. ISO/PAS 28000シリーズ

**認定機関** (Accreditation body)

ISO/IEC 17011

**適合性認証機関** (監査・認証)

ISO 28003

**各種会社事業所等**

ISO  
28000

ISO 28004

ISO  
20858

ISO  
28001

その他  
の規格

### 3. ISO/PAS 28000シリーズ

## ISO/IEC 17011:2004

### 適合性評価

適合性評価機関の認定を行う認定機関に対する  
一般的要求事項

### Conformity assessment

General requirements for accreditation bodies accrediting  
conformity assessment bodies

### 海上脱出設備の通信手段

Marine Evacuation System

Means of Communication



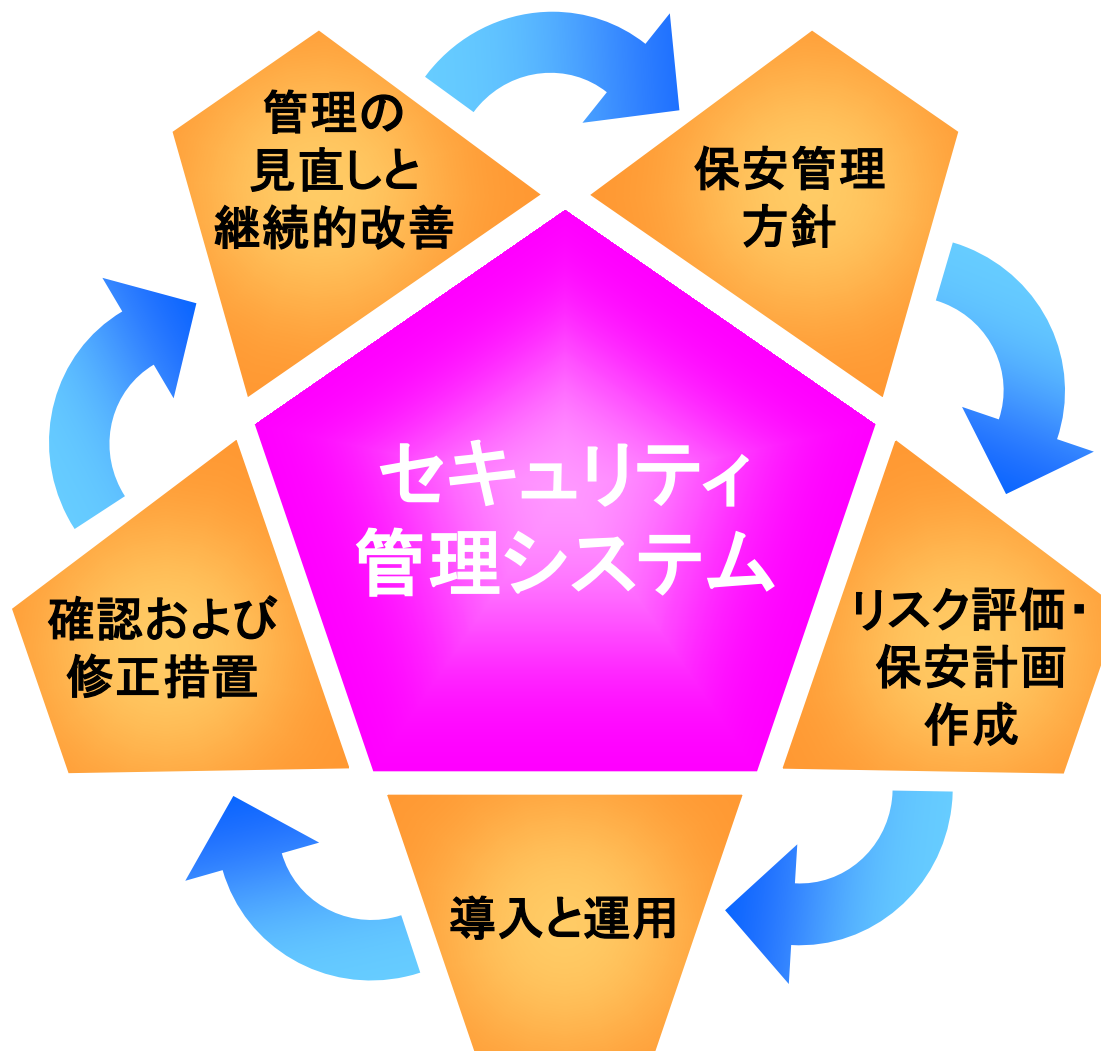
## 4. ISO/PAS 28000 & 28004

### ISO/PAS 28000:2005

- ISO 14001:2004をベースに作成
- PDCAサイクルを要求
  - Plan : ポリシーに沿って、目標と手順を決める
  - Do : 手順を実施する
  - Check : 実施状況をポリシー、目標等に沿って  
点検し、報告する
  - Action : 管理システムを継続的に改善する

## 4. ISO/PAS 28000 & 28004

### ISO/PAS 28000:2005



## 4. ISO/PAS 28000 & 28004

- 4.1 一般要件
- 4.2 保安管理方針
- 4.3 リスク評価・保安計画の作成
  - 4.3.1 セキュリティリスク評価
  - 4.3.2 規則等の確認・遵守
  - 4.3.3 セキュリティ管理の目的の明確化
  - 4.3.4 セキュリティ管理の目標設定
  - 4.3.5 保安管理プログラム

## 4. ISO/PAS 28000 & 28004

### ■ 4.4 導入と運用

- 4.4.1 構造・権限・責任の明確化
- 4.4.2 能力・訓練・認識力
- 4.4.3 連絡
- 4.4.4 文書化
- 4.4.5 文書とデータの管理 (control)
- 4.4.6 運用の管理 (operational control)
- 4.4.7 非常時の準備・対応および保安の復旧

## 4. ISO/PAS 28000 & 28004

### ■ 4.5 確認および修正措置

● 4.5.1 保安能力の判定

● 4.5.2 システムの評価

● 4.5.3 装置の故障等問題点への対応と予防

● 4.5.4 記録の管理

● 4.5.5 監査（自己監査）

### ■ 4.6 管理の見直しと継続的改善



## 4. ISO/PAS 28000 & 28004

### ISO/PAS 28004の構成

ISO/PAS 28000:2005の各節毎に以下を示す

- a) ISO/PAS 28000:2005の要件 (Requirement)
- b) 意図 (Intent)
- c) 考慮すべき項目/情報 (Typical Input)
- d) 実施方法 (Process) ≒ 検討項目
- e) 典型的な実施結果 (typical Output)

## 4. ISO/PAS 28000 & 28004

### ISO/PAS 28004の構成

◆ 目次、前書き、付録を除く本文	: 約16,000語
■ 1 目的 (Scope)	: 約300語
■ 2 参考文献書 (Reference publications)	: 約75語
■ 3 用語と定義 (Terms and definitions)	: 約550語
■ 4 保安管理システムの要素 (Elements)	: 約15,000語
● 4.1 一般要件	: 約370語
● 4.2 ポリシー	: 約1,030語
● 4.3 評価と計画	: 約4,000語
● 4.4 導入と運用	: 約4,170語
● 4.5 確認と修正	: 約4,780語
● 4.6 見直しと継続的改善	: 約700語

## 4. ISO/PAS 28000 & 28004

### ISO/PAS 28000 & 28004

4.2 ポリシーの決定

4.3 評価

4.3 計画の策定

4.4 計画の実施

4.5 確認と修正

4.6 見直しと継続的改善

### ISPS Code

(1) 責任者の決定

(2) 評価

(3) 計画の策定

(4) 計画の実施

(5) 再評価・継続的改善

(6) 装置の設置

## 5. ISO/PAS 28001

### 新項目提案時の表題

**サプライチェーンセキュリティ保護の実務**

(Best Practices for Custody in Supply Chain Security)

### 最終会議終了時点の表題

**サプライチェーンセキュリティの管理、評価、および計画の実施  
－ 要件と指針**

(Specification for implementing supply chain security management, assessments and plans – Requirements and guidance)

### ISO中央事務局により修正された表題

**サプライチェーンの保安のための実務**

**－ 評価と計画**

(Specification on Best Practices for Implementing Supply Chain Security, assessment and plans)

## 5. ISO/PAS 28001

### 1 Introduction

「国際サプライチェーン」および要素の適切な水準の  
保安の実施を可能にする

- 保安対策でカバーする範囲を明確にする
- 保安評価（脆弱性評価）の実施
- 保安計画の作成
- 訓練プログラムの設定

### 2 用語と定義

### 3 スコープ

## 5. ISO/PAS 28001

### 4 保安対策でカバーする範囲 (Scope of coverage)

- ビジネスパートナー（下請け等関係者）のうち、保安対策上の関係者の範囲を決める
- ビジネスパートナーの保安の見直し
- 関係するビジネスパートナーからは、「保安に関する申告/宣言」(security declaration)を受け取る

### 同等性の見なし規定

ISPS Code等の国際的に承認された保安対策を実施している運輸事業者 (Transportation companies and facilities) は、この仕様の要件を満たす

## 5. ISO/PAS 28001

### 5 保安プロセス (Supply Chain Security Process)

- 5.1 保安評価のスキープの決定
- 5.2 保安評価の実施
  - 5.2.1 評価実施者/チーム
  - 5.2.2 評価プロセス
- 5.3 保安計画の作成
- 5.4 保安計画の実施
- 5.5 保安プロセスの実施状況把握および実施
- 5.6 保安上の問題 (security incident) 発生の際の措置
- 5.7 保安上の情報の保護

## 5. ISO/PAS 28001

### Informative Annex A

#### サプライチェーン保安プロセス

- 保安プロセスの説明（やや具体的）
- 保安の現状把握のためのチェックリスト  
(Performance Review List: 31項目)
- 脅威 (thereat) シナリオのリスト

### Informative Annex B

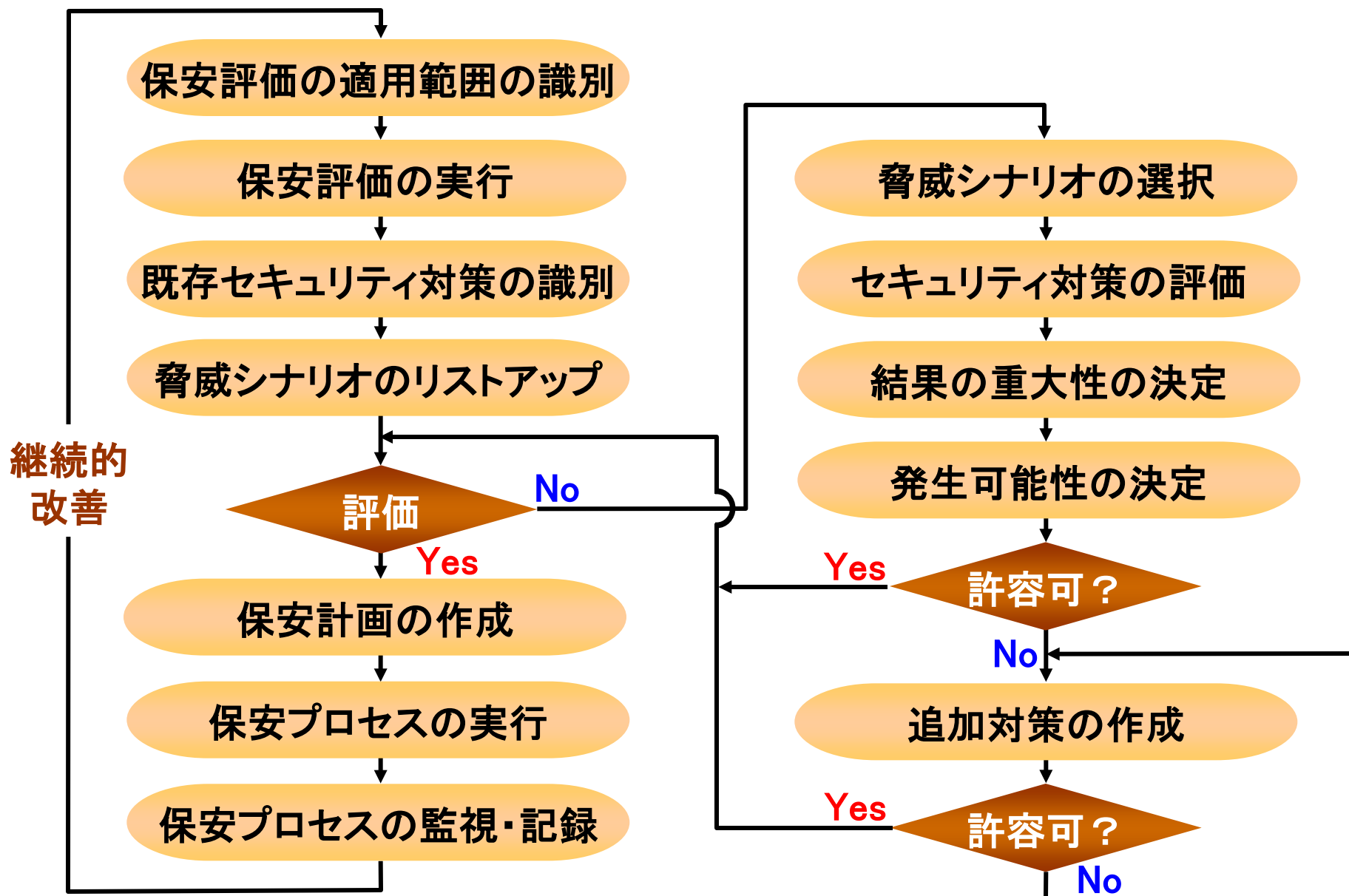
#### 保安リスク評価および保安対策開発の方法論

### Informative Annex C

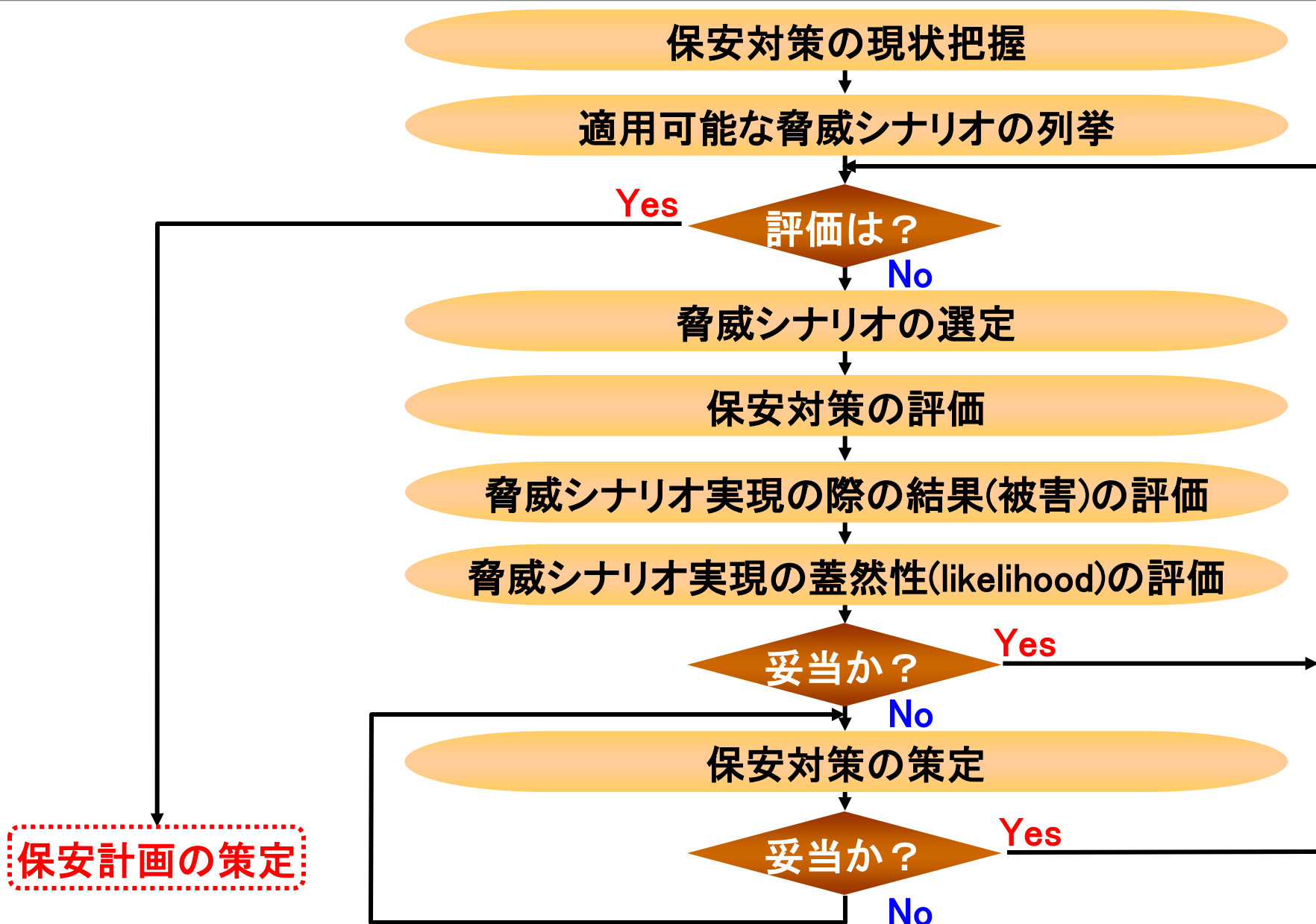
#### 助言および審査の指針



# 5. ISO/PAS 28001 サプライチェーン保安プロセス



# 5. ISO/PAS 28001 サプライチェーン保安評価法



## 6. ISO/PAS 28003

ISO適合性評価委員会 (Committee on Conformity Assessment) で、監査・認証機関の要件を策定中

- ISO/IEC規格案17021 適合性評価  
ーマネジメントシステムの監査および認証を提供する機関  
に対する要求事項

(Conform assessment – Requirements for bodies providing audit and certification of management systems)



- ISO/PAS 28003 保安管理システム  
ーサプライチェーン保安管理システムの監査および認証を  
提供する機関の要件

(Security management systems – Requirements for bodies providing audit and certification of supply chain security management systems)

## 6. ISO/PAS 28003

- 4 認証機関の原則 (Principles for certification bodies)
  - 4.1 一般 (General)
  - 4.2 公平性/不偏性 (Impartiality)
  - 4.3 力量/能力/適格性 (Competence)
  - 4.4 責任/信頼性 (Responsibility)
  - 4.5 公開/透明性 (Openness)
  - 4.6 機密性/守秘性 (Confidentiality)
  - 4.7 苦情の解決 (Resolution of complaints)

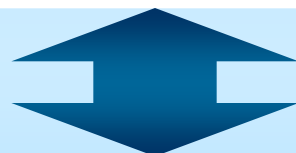
### ■ 4.2～4.7 第三者認証機関の六原則

監査において知り得た情報の悪用防止の要件は？  
監査関係者の人物証明 (Security Clearance) は？

## 6. ISO/PAS 28003

### 第三者認証の適否の判断

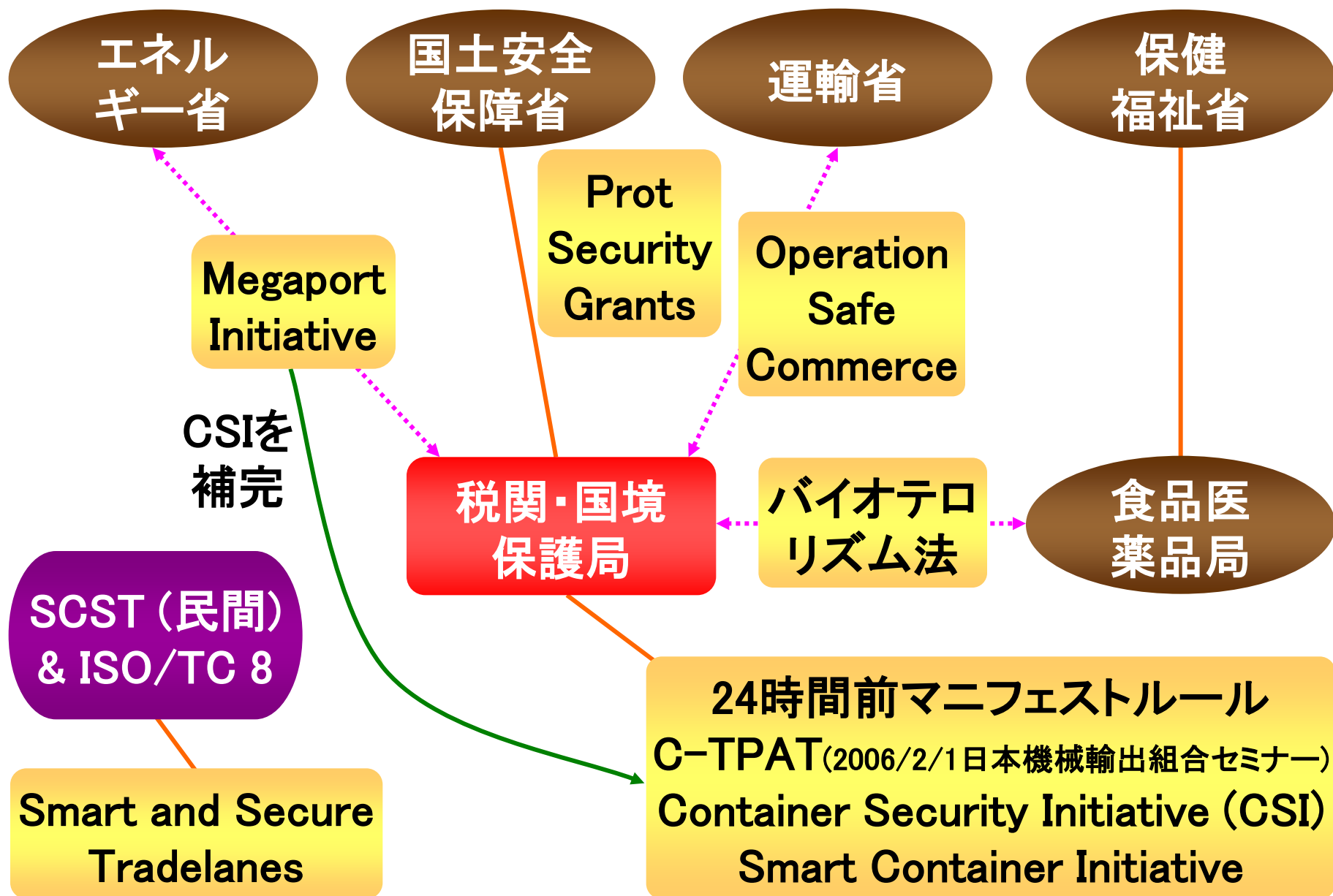
- Securityにおける重要事項: **Access control**
- 第三者機関による監査 : **外部への情報開示**



- 組織内部の検討だけで十分？
- 外部へのアピールは？

保安対策の確保は、営業上の強みとなり得るのか？

# 7. セキュリティーに関する国際(米国)動向



## 7. セキュリティーに関する国際動向

### 世界税関機構(WCO)

- 税関手続きの簡素化および調和に関する国際規約の改正議定書（改正京都条約）
  - Risk Control: 通関の際は、貨物を全部検査するのではなく、危険性の高い貨物を高い比率で調べる(危険性の低い貨物は調べない)
- 国際貿易の安全性確保および円滑化のための「基準の枠組み」  
(Framework of Standards to Secure and Facilitate Global Trade)
  - **Authorized Economic Operator : AEO**

**ご清聴、ありがとうございました。**