米国C-TPAT 輸出者プログラムの資格要件について

2014年8月
日本機械輸出組合

Customs-Trade partnership Against Terrorism (C-TPAT)

輸出者の要件

輸出者C-TPAT

当初よりC-TPATはバン詰の場所から米国最初の到着港に至るまで、国際サプライチェーン全体のサプライチェーンセキュリティ向上を追求してきた。C-TPATプログラムは進化し続け、輸出者も国際サプライチェーンにおいて重要な役割を持っていることが明らかになってきたが、米国CBPが大部分を管掌している分野ではなかった。C-TPATの輸出コンポーネントを発展させることでC-TPATはプログラムとして、また海外の相互承認税関当局との相互承認関係の更なる向上につながるだろう。

定義

C-TPATでは、輸出者は次のように定義される。

輸出業務に関わる当事者である個人または法人であって、米国外への貨物の送り出しについて決定、管理の権限、責任を有する者。

輸出事業者の資格要件

C-TPAT輸出プログラムへの参加希望者は、プログラムが定義する輸出者であることに加え、次の資格要件を満たしていなければならない。

1. 米国以外へ輸出する既存の米国輸出者であること
2. 米国に事務所があること
3. a.従業員登録番号（EIN）または b. Dun & Bradstreet (DUNS)番号で文書登録されている既存の米国輸出者であること
4. 文書化された輸出セキュリティプログラムがあり、C-TPATプログラムのメインコンタクトポイントとして指名を受けた役員またはマネージャーがいること。さらに指名を受けたコンタクトポイントが対応できない時には、代わりのコンタクトポイントがいること
5. C-TPAT輸出者合意書に書かれたC-TPATサプライチェーンセキュリティ基準の保持にコミットしていること
6. 輸出者がC-TPAT輸出者のセキュリティ基準を満たせるよう、いかに社内基準を合致させ、維持し、向上しているかを示すC-TPATサプライチェーンセキュリティプロファイルを作成し、CBPに提出していること
7. 資格者となるため、輸出者の直近12か月間の輸出報告順守度が許容レベルにあり、商務省、国務省、財務省、原子力規制委員会、麻薬取締局、国防総省といった米国の規制当局との関係が良好でなければならない。

輸出者セキュリティの最小基準

C-TPATでは国際サプライチェーンの複雑さを理解しており、輸出者のリスク分析に基づくセキュリティ対策の適用、導入を認めている。このためこのプログラムはメンバーのビジネスモデルを踏まえ、セキュリティ計画に柔軟性を持たせ、カスタマイズすることを認めている。

本資料に記載されているように適切なセキュリティ対策を、C-TPAT輸出参加者のサプライチェーンに導入し、また維持しなければならない。

輸出者は、以下のC-TPATセキュリティ基準を踏まえ、国際サプライチェーンの包括的なリスク評価を行わなければならない。

輸出者が倉庫、ロジスティクスプラロバイダー、船社やその他の輸出サプライチェーンの構成要素等、自社のサプライチェーンの一部をアウトソースするとか、契約にしている場合には、輸出者は確実に効果的なセキュリティ対策を整え、サプライチェーン全体に施せるよう、取引先と協働しなければならない。

取引先要件

輸出者はサービスプロバイダー、製造者、製品のサプライヤー、ベンダー等、取引先のスクリーニングと選定プロセスを文書化し、検証できるようにしなければならない。

できれば、このプロセスの中に、商務省・産業安全保障局(BIS)、国務省・国防貿易管理局(DDTC)、財務省・海外資産管理局（OFAC）のチェックリストを入れておかなければならない。

禁止リストに記載されている場合には出港の24時間前までに、SCSSや関連の機関に報告されなければならない。

Customs-Trade Partnership Against Terrorism (C-TPAT)

Exporter Eligibility Requirements

C-TPAT Exporter

Since its inception, the Customs-Trade Partnership Against Terrorism (C-TPAT) program has sought to enhance supply chain security throughout the international supply chain, from point of stuffing, through to the first U.S. port of arrival. As the C-TPAT program has continued its evolution, it has become apparent that exports also have an important role in international supply chains and while this sector is not as heavily owned by U.S. Customs and Border Protection (CBP) and the C-TPAT program, developing an export component for C-TPAT would further enhance both the program and its relationship with other mutually recognized Foreign Customs administrations.

Definition

For C-TPAT purposes, an exporter is defined as:

A person or company who, as the principal party in interest in the export transaction, has the power and responsibility for determining and controlling the sending of the items out of the United States.

Exporter Entity Eligibility Requirements

Entities that wish to participate in the C-TPAT Exporter program must meet with the program's definition of an Exporter as well as meet with the following eligibility requirements:

1. Be an active U.S. Exporter out of the United States.
2. Have a business office staffed in the U.S.
3. Be an active U.S. Exporter with a documentable
   a. Employee Identification Number (EIN),
   or
   b. Dun & Bradstreet (DUNS) number,
4. Have a documented export security program and a designated officer or manager who will act as the C-TPAT program main point of contact. Additionally the participant should have an alternate point of contact should the designated point of contact be unavailable.
5. Commit to maintaining the C-TPAT supply chain security criteria as outlined in the C- TPAT Exporter agreement.
6. Create and provide CBP with a C-TPAT supply chain security profile which identifies how the Exporter will meet, maintain, and enhance internal policy to meet the C-TPAT Exporter security criteria.
7. In order to be eligible the Exporter must have an acceptable level of compliance for export reporting for the latest 12-month period and be in good standing with U.S. Regulatory Bodies such as: Department of Commerce, Department of State, Department of Treasury, Nuclear Regulatory Commission, Drug Enforcement Administration, and Department of Defense.

Exporter Minimum Security Criteria

C-TPAT recognizes the complexity of international supply chains and endorses the application and implementation of security measures based upon risk analysis by exporters. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Appropriate security measures, as listed throughout this document, must be implemented and maintained throughout the above C-TPAT export participants' supply chains. Exporters must conduct a comprehensive risk assessment of their international supply chain based upon the following C-TPAT security criteria. Where an exporter outsources or contracts elements of its supply chain, such as to a warehouse, logistics provider, carrier or other export supply chain element, the exporter must work with these business partners to ensure that effective security measures are in place and adhered to throughout the entire supply chain.

Business Partner Requirements

Exporters must have written and verifiable processes for the screening and selection of business partners including service providers, manufacturers, product suppliers, and vendors. Where applicable, these processes must include checks against the Department of Commerce/Bureau of Industry and Security (BIS), Department of State/Directorate of Defense Trade Controls (DDTC), and Department of Treasury/Office of Foreign Assets Control (OFAC) lists. Entities on prohibited lists should be reported to the SCSS and relevant authority within 24 hours prior to departure.

米国C-TPAT 輸出者プログラムの資格要件について

セキュリティ手順

取引先をスクリーニングするために文書化した手続きがなくてはならず、これによって特定の要因や慣行が分かり、輸出者が追加的な検査を行うトリガーとなる。

取引先がC-TPA対象業種であれば（輸入者、船社、港湾、ターミナル、ブローカー、混載業者等）、輸出者は取引先がC-TPATの承認を受けているか、受けていないか、および・または　相互関係にあるAEOプログラムの参加者（AEO認定）かどうかを示した書類を作成しなければならない。（例、SVI番号等）

取引先がC-TPAT、またはAEOプログラムの対象業種でない場合、輸出者は取引先にC-TPATセキュリティ基準を満たしていることを示すよう文書または電子的手段で確認要請しなければならない**。**

（契約上義務：取引先の上級役員からコンプライアンスを証明するレターを出す、

取引先から彼らのコンプライアンスがC-TPATセキュリティ基準にあるとか、海外の税関当局によって管理されている同等のAEOセキュリティプログラムであるとかを示す供述書をまとめる、輸出者セキュリティアンケートを回答する等）

リスクアセスメント手順を文書化することで、C-TPATに適合しない取引先はC-TPATセキュリティ基準の順守を輸出者に証明しなければならない。

会社の輸出プログラムのリスクアセスメントは、毎年行わなければならない。

起点

輸出者は取引先に対して、輸出地点での出荷のインテグリティを高めるため、C-TPATのセキュリティ基準に沿うセキュリティプロセスと手順を通知しなければならない。

輸出者が要求するセキュリティ標準が維持できるよう、取引先の手順および施設をリスクに応じて定期的に点検しなければならない。

外国税関当局のサプライチェーンセキュリティプログラムへの参加、認証

既存の取引先または見込み取引先で、外国税関当局が管理しているサプライチェーンセキュリティプログラムの認証を得ている場合は、輸出者に参加ステータスを通知しなければならない。

その他、選定の内部基準

財務健全性、契約上のセキュリティ要件への適合力、セキュリティの欠如を認識し必要に応じて、修正する能力等、内部要件は輸出者が申し入れなければならない。

内部要件は経営者がリスクベースの書類を用いて評価しなければならない。

コンテナセキュリティ

許可を受けていない機材や人の侵入を防げるよう完全性（インテグリティ）を保たなければならない。

バン詰めを行う場所では、文書化した手続きで出荷コンテナのシールを適切に行い、完全性が保てるようにしなければならない。

コンテナ検査

バン詰めの前に、ドアのロック構造の信頼性を含めてコンテナ構造の物理的なインテグリティを確認する手順が取られていなければならない。いずれのコンテナにも7ポイント検査手順を勧める。

- 前壁
- 左側
- 右側
- 床面
- 天井 / 屋根
- 内側 / 外側 ドア、ドア金具、留め具
- 外側 / 車台

コンテナシール

輸出コンテナのシールは、シールを常に完全な状態に置くことを含め、安全なサプライチェーンにおいて重要な要素であり、今なお輸出者がC-TPATへコミットする上で欠かせない部分である。

米国から輸出用に積み込まれた全てのコンテナには高度なセキュリティシールを取り付けなければならない。

いずれのシールも高度なセキュリティシールとしては現行のISO17712の同等以上でなければならない。

手順書を文書化し、どのようにシールをコントロールするか、船積みする輸出コンテナにどのように取り付けるか、シール及び/またはコンテナの故障を認識し、CBPまたは海外の関係当局へ報告する手順も含めて、規定しなければならない。

特に指定された社員だけが完全性を目的として、シール配布を行うようにしなければならない。

Security procedures

Written procedures must exist for screening business partners, which identify specific factors or practices, the presence of which would trigger additional scrutiny by the exporter.

For those business partners eligible for C-TPAT certification (importers, carriers, ports, terminals, brokers, consolidators, etc.) the exporter must have documentation (e.g., SVI number) indicating whether these business partners are or are not C-TPAT certified and/or participating in a reciprocal Authorized Economic Operator (AEO) program (e.g., AEO certificate).

For those business partners not eligible for C-TPAT certification or participation in an AEO program, exporters must require their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation (e.g., contractual obligations; via a letter from a senior business partner officer attesting to compliance; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria or an equivalent AEO security program administered by a foreign customs authority; or, by providing a completed exporter security questionnaire). Based upon a documented risk assessment process, non-CTPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the exporter.

Risk assessments of the company's export program must be completed on an annual basis.

Point of Origin

Exporters must inform business partners of security processes and procedures that are consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of export.

Periodic reviews of business partners' processes and facilities should be conducted based on risk to maintain the security standards required by the exporter.

Participation/Certification in Foreign Customs Administrations Supply Chain Security Programs:

Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the exporter.

Other Internal Criteria for Selection

Internal requirements, such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed, should be addressed by the exporter.

Internal requirements should be assessed by management utilizing a risk-based document.

Container Security

Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.

At point of stuffing, written procedures must be in place to properly seal and maintain the integrity of the shipping containers.

Container Inspection

Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors, door hardware, and fasteners
- Outside/Undercarriage

Container Seals

The sealing of export containers, to include continuous seal integrity, are crucial elements of a secure supply chain, and remains a critical part of an exporter's commitment to C-TPAT.

A high security seal must be affixed to all loaded containers destined for export from the U.S.

All seals must meet or exceed the current ISO 17712 standards for high security seals.

Written procedures must stipulate how seals are to be controlled and affixed to loaded export containers to include procedures for recognizing and reporting compromised seals and/or containers to CBP or the appropriate foreign authority.

Only designated employees should distribute seals for integrity purposes.

米国C-TPAT 輸出者プログラムの資格要件について

コンテナ保管場所
コンテナは、不正アクセス　及び/または 操作を防ぎ、コンテナの完全性を確実に維持し、特に許可していない物質の侵入を防ぐため、安全な場所で保管しなければならない。

コンテナ及びコンテナ保管場所への不正侵入、輸出用コンテナの中で見つかった秘密の隠し場所等、構造上の変更についての報告および無害化について手順で定めなければならない。
通知は発見から24時間以内に特定のサプライチェーンセキュリティスペシャリスト(SCSS)へ行うこと。

船舶のトラッキング、モニタリング手順
輸出者は輸送プロバイダーが次のようなトラッキング、モニタリング手順を確実に順守するようにしなければならない。

貨物の輸出地点までの輸送の間は、輸送容器およびコンテナの完全性は保たれていること。 トラッキングおよびモニタリング活動のログ又は、同等の技術の利用が求められる。ドライバーのログが使われるのであれば、トレーラー/コンテナの完全性が確認されていることを示さなければならない。

事前に決めたルートがあれば、輸送プロバイダーは輸出者に確認しておかなければならない。この手順には、輸送プロバイダーのランダムルートチェックに加え、ピークタイム、ノンピークタイムにおける、積み込み地点 / トレーラーピックアップ場所、輸出地点、及び/または 配送先との間の時間の長さについての文書化、検証を入れておかなければならない。
ドライバーは、天候、交通量及び/またはルート切り替え等によるルート遅延について、運行管理者に通知しなければならない。

輸送プロバイダーの経営者は 文書化された、抜き打ち検査を定期的に実施し、ログがメンテされ、輸送容器のトラッキング、モニタリング手順に沿って実施されているのを確認しなければならない。

ドライバーは輸送容器、コンテナに何らかの異常や、特異な構造上の修正を発見した場合は、報告し、文書にしておかなければならない。

物理的なアクセスコントロール

アクセスをコントロールすることで、貨物施設への不正侵入を防止し、従業員、来訪者のコントロールを維持し、企業財産を守ることができる。アクセスコントロールでは、入場できる全ての場所で、全ての従業員、来訪者、サービスプロバイダー、ベンダーの身元確認を行わなければならない。
従業員とサービスプロバイダーは、正当に仕事が行える場所だけに出入りすることができるようにしなければならない。

従業員： 従業員識別システムは身元確認および出入り管理目的に用意しなければならない。
従業員には業務遂行に必要な保安エリアに限って出入りできるようにしなければならない。会社の経営者およびセキュリティ担当者は、従業員、来訪者、ベンダーのIDバッジの配布、抹消を適切にコントロールしなければならない。入場用器具（カギ、キーカード等）の発行、抹消、変更に関わる手順は文書化しておかなければならない。

来訪者/ベンダー/サービスプロバイダー： 来訪者は記録のため、写真IDを来訪時に提示しなければならない。来訪者は全員エスコートされ、来客用IDが発行され、見えるように身に着けさせなければならない。

許可のない人の対応、排除： 許可されていない/見知らぬ人を認識し、確認し、排除する手続きをとらなければならない。

配送（郵便物を含む）
運送プロバイダーは到着時に、適切なID及び/または写真つきIDを記録上、提示しなければならない。着荷および郵便物は社内配送前に定期的に検査しなければならない。

社員のセキュリティ
内定者の身元検査、現行の社員の定期チェックを手続として行わなければならない。

雇用前審査：履歴書などの申請情報は雇用前に検証されなければならない。

バックグラウンドチェック/調査： 連邦、州および地元の規則に従い、内定者に対してはバックグラウンドチェックと調査を行わなければならない。
一度雇用した後は、原因及び/または 従業員の立場への配慮を踏まえて、定期検査、再調査を行わなければならない。

従業員解雇手続き：会社は退職した社員に対しては、ID、施設、システムへのアクセスを抹消するための手続きを整えておかなければならない。

Container Storage
Containers must be stored in a secure area to prevent unauthorized access and/or manipulation and to ensure container integrity is being maintained, especially to protect against the introduction of unauthorized material.

Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas and any structural changes, such as a hidden compartment, discovered in containers destined for export. Notification should be made within 24 hours of discovery to the assigned Supply Chain Security Specialist (SCSS).

Conveyance Tracking and Monitoring Procedures
Exporters should ensure that their transportation providers adhere to the following tracking and monitoring procedures:

Conveyance and container integrity is maintained while the conveyance is en route transporting cargo to the point of export. Utilizing a tracking and monitoring activity log or equivalent technology is required. If driver logs are utilized, they should reflect that trailer/container integrity was verified.

Predetermined routes should be identified by the transportation provider for the exporter, and these procedures should consist of random route checks by the transportation provider along with documenting and verifying the length of time between the loading point/trailer pickup, the export point, and/or the delivery destinations, during peak and non-peak times.
Drivers should notify the dispatcher of any route delays due to weather, traffic and/or rerouting.

Transportation provider management must perform a documented, periodic, and unannounced verification process to ensure the logs are maintained and conveyance tracking and monitoring procedures are being followed and enforced.

Drivers must report and should document any anomalies or unusual structural modifications found on the conveyance or container.

Physical Access Controls

Access controls prevent unauthorized entry to cargo facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers and vendors at all points of entry. Employees and service providers should only have access to those areas of a facility where they have legitimate business.

Employees: An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification
badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.

Visitors/Vendors/Service Providers: Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and provided temporary identification that must be visibly displayed on their person.

Challenging and Removing Unauthorized Persons: Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Deliveries (including mail):
Proper ID and/or photo identification must be presented for documentation purposes upon arrival by transportation providers. Arriving packages and mail should be periodically screened before being disseminated.

Personnel Security
Processes must be in place to screen prospective employees and to periodically check current employees.

Pre-Employment Verification: Application information, such as employment history and references must be verified prior to employment.

Background checks / investigations: Consistent with, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

Personnel Termination Procedures: Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

米国C-TPAT 輸出者プログラムの資格要件について

手順化したセキュリティ
サプライチェーン上、貨物の輸送、荷捌き、保管に関連するプロセスの完全性、セキュリティの確保を確実に行えるよう、セキュリティ対策を取らなければならない。

輸送貨物への接近を制限するようなセキュリティ手順を導入しなければならない。この手順で、合衆国から輸出する前に国内ロケーションの施設からの輸送途上で輸出禁制品は船積みできないようにする。

貨物の不一致： 不足、過剰、その他著しい不一致、異常があった場合は、適切に解決しまたは調査しなければならない。

不法または不審な活動が発見された場合は、税関、特定のサプライチェーンセキュリティスペシャリスト、及びまたは 他の関連する法律実施機関に対して適切に通知しなければならない。

文書化手順： 手順上、商品/ 貨物の輸出準備に使われるいずれの情報も (EEI、その他要求された輸出フォームで)、読みやすく、完璧で、正確であり、情報誤りの変更、消去、導入ができないよう確実に保護されていなければならない。

船荷証券/航空運送状/マニフェスト手順： 輸出貨物の完全性を確保できるよう、取引先との間の情報は正しくタイムリーに送受信されるような手順でなければならない。

船積:輸出貨物は正しく内容説明され、計量、ラベル、マーク、個数を表記し、点検しなければならない。
出荷貨物は、注文書や配送指示書と照合しなければならない。貨物の受け取り、引き渡しを行う前に貨物の受け渡しを行うドライバーの身元確認を行わなければならない。

禁止、制限を受けている者の検査： 文書化した手続き、手順で、国務省/DDTC、商務省/BIS、財務省/OFACのdenied personリストにある者を確認し、および輸出取引を拒否しなければならない。禁止リストに記載された者についてはSCSSおよび関連当局に出港前24時間以内に通知しなければならない。

物理的セキュリティ
登録されていない物質、無許可の者を防止、検出、抑止し、コンテナへの潜伏を含めて輸送器材に入り込まないような手順がとられなければならない。

国内の場所で貨物の取扱い及び貯蔵する施設には物理的な障壁を設け、不法侵入を防止する障害物を置かなければならない。ビジネスモデル次第で、輸出者は以下のようなC-TPATの物理セキュリティ基準を実践的かつ適切なものとしてサプライチェーン全体に取り込まなければならない。

フェンス： 荷捌き場および倉庫施設周りのエリアは境界フェンスで囲まなければならない
荷捌きを行う構造物内の室内フェンスで、国内、国際、高価値、危険物と貨物を区分しなければならない。いずれのフェンスも、完全性と損傷について、定期的に検査しなければならない。

門扉(gate)および守衛所(gate house)： 車両 及び/または 人が出入りする門扉には要員を配置し監視しなければならない。門扉の数は出入りと安全上で適切な範囲で、必要最小限度にしておく。

駐車場： プライベートの乗用車は荷捌き場および倉庫に隣接する場所に駐車させてはならない。

建物の構造： 建物は不法侵入に耐えうる素材で建築されていなければならない。定期的に点検、修繕し、構造上、完全性が保たれるようにしなければならない。

ロック装置とカギ制御： 外部および内部の窓、門扉、フェンスは全て、ロック装置を取り付け安全にしなければならない。経営者およびセキュリティ要員はロック及びカギの発行を全てコントロールしなければならない。

照明： 施設の内部、外部には必要な照明を設置しなければならない。その設置場所には、次のようなエリアが含まれる。： 出入り口、荷捌き場、保管場所、フェンスライン、駐車場。

警報システムおよびビデオ監視カメラ： 施設をモニターし、荷捌き場、保管場所を不法侵入から守るため、警報システム及びビデオ監視カメラを利用しなければならない。

Procedural Security
Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

Security procedures should be implemented that restrict access to the export shipment. The procedures should prevent the lading of contraband while en-route from facilities in domestic locations prior to export from the United States.

Cargo Discrepancies: All shortages, overages, and other significant discrepancies or anomalies must be resolved and or investigated appropriately.

Customs, the assigned Supply Chain Security Specialist and or other appropriate law enforcement agencies, must be notified if illegal or suspicious activities are detected-as appropriate.

Documentation Processing: Procedures must be in place to ensure that all information used in the preparation of merchandise/cargo for export (EEI or other required export form), is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

Bill of Lading/Airway Bill/Manifesting Procedures: To help ensure the integrity of cargo being exported, procedures must be in place to ensure that information transmitted/received to/from business partners is reported accurately and timely.

Shipping: The export cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

Screening for Prohibited or Restricted Parties: Documentable procedures and processes must exist to identify any party on lists from State/DDTC, Commerce/BIS or Treasury/OFAC denied persons and who are involved in an export transaction with the exporter. Entities on prohibited lists should be reported to the SCSS and relevant authority within 24 hours prior to departure.

Physical Security
Procedures must be in place to prevent, detect, or deter undocumented material and unauthorized personnel from gaining access to conveyance, including concealment in containers.

Cargo handling and storage facilities in domestic locations should have physical barriers and deterrents that guard against unauthorized access. Exporters should, according to their business models, incorporate the following C-TPAT physical security criteria throughout their supply chains as practical and appropriate.

Fencing: Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage.

Gates and Gate Houses: Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

Parking: Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

Building Structure: Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

Locking Devices and Key Controls: All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

Lighting: Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

Alarms Systems & Video Surveillance Cameras: Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

米国C-TPAT 輸出者プログラムの資格要件について

輸出教育と脅威認識

C-TPAT輸出者は輸出セキュリティプログラムを文書化し、C-TPATプログラムの連絡担当者となる役員またはマネージャーを指名しておかなければならない。このプログラムは社員への連絡体制に見られる会社の組織構造にいたるまでサポートしておく必要がある。

サプライチェーンで輸出の最終ポイントを含めあらゆる場所で不法な活動によって引き起こされる脅威を認識し、意識を育てるようにするため、脅威認識のプログラムを作り、継続しなければならない。輸出セキュリティの役員やマネージャーがどのように規則や手順の変更にかかる情報を受け取るか、手順を文書化しておかなければならない。

社員は、セキュリティの事件や疑いに対して取組み、またどのように報告するか、会社の手順を理解しておかなければならない。

出荷、荷受けのためのエリア、郵便物の受け取り、開封を行う場のように重要な輸出の場所においては、社員に対して追加的な教育を行わなければならない。

さらに、貨物の完全性の維持、内部謀略の認識、入室管理の防護、物理的セキュリティの向上のために社員の助けとなるような特別な教育を行わなければならない。

こうした教育は関係社員の参加インセンティブとなる。

情報技術セキュリティ

パスワード保護： 自動システムであれば、個別に割り当てられたアカウントを使用し、定期的にパスワードの変更を要求するものでなければならない。

ITセキュリティの方針、手順、標準を整備し、教育という形で社員に伝えられなければならない。

説明責任 不正アクセスを含むITの乱用、ビジネスデータの改ざん、変更をシステムで認識できるようにしなければならない。いかなるシステム妨害も、乱用した場合には適切な懲罰が課されなければならない。

Export Training and Threat Awareness

A C-TPAT Exporter must have a documented export security program as well as a designated officer or manager who will act as the C-TPAT program point of contact. This program should have support throughout the corporate structure of the company displayed in correspondence to personnel.

A threat awareness program should be established and maintained to recognize and foster awareness of the threat posed by illegal activities at each point in the supply chain, to include final point of export. There should be documented procedures on how the export security officer or manager receives information about changes in regulations or procedures.

Employees must be made aware of the procedures the company has in place to address a security incident or suspicion thereof and how to report it.

Additional training should be provided to employees in vital export areas such as the shipping and receiving areas, as well as those receiving and opening mail.

Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, protecting access controls and enhancing physical security.

These programs should offer incentives for active employee participation.

Information Technology Security

Password Protection: Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training.

Accountability: A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.