日本機械輸出組合　仮訳

C-TPAT 立入検査プロセス・ガイドライン

C-TPAT VALIDATION PROCESS GUIDELINES(2003 年 1 月 23 日)

事務局注：
正しくは米国関税庁の原文をご参照下さい。
http://www.customs.treas.gov/ImageCache/cgov/content/import/commericial_5fenforcement/ctpat/validation_5fprocess/validation_5fprocess_5fguidelines_2epdf/v1/validation_5fprocess_5fguidelines.pdf

---

I.　イントロダクション

C-TPAT 参加者がそれぞれのセキュリティ・プロフィールおよび税関へ提出している追加情報に述べられているセキュリティ措置を実行していることを確保するために、米国関税庁は立入検査プロセスを開発してきた。立入検査プロセスは米国税関担当官と参加企業の担当者によって共同して実施されるものである。立入検査は、C-TPAT 参加者のセキュリティ・プロフィールの内容（Material）および当該参加者によって提出された関連資料に焦点を当て、C-TPAT の指導パートナーシップ原則に従って実施される。

II.　目的

立入検査の目的は、C-TPAT 参加者のセキュリティ・プロフィールに述べられているサプライチェーン・セキュリティ措置が実施されていることを確実にすることにある。企業のオペレーションと C-TPAT セキュリティ・リコメンデーションからの観点に立って、立入検査チームは、C-TPAT 参加者のプロフィールの中でキーとなるセキュリティ措置の状態と有効性を評価し必要な場合には勧告を行う。

III.　立入検査の原則

C-TPAT プログラムの指導原則はパートナーシップである。C-TPAT プログラムはボランタリーであり、テロリスト及びテロリスト組織によって危険に晒されないようサプライチェーンを守る情報を共有するべく作られている。

立入検査プロセスは、米国税関と C-TPAT 参加者が共同して、当該参加者の C-TPAT セキュリティ・プロフィールに規定されているセキュリティへの取組みが確実に効果的に実施されようセキュリティ・プロフィールを見直すことができるようにするものである。このプロセスを通じて、セキュリティ問題を議論し、国際サプライチェーンの安全確保という究極の目的に向けたベスト・プラクティスを共有する機会がもたらされることにもなるだろう。

C-TPAT 立入検査は監査ではない。加えて、立入検査は簡潔なものであり、10 稼働日を越える長さで行なわれることはないであろう。

参加者の C-TPAT セキュリティ・プロフィール及び（米国税関の）立入検査チームの韓国に基いて、米国関税庁本庁はまた、特定のセキュリティ・エレメントが検査されるよう監督することになる。

IV. 立入検査の実施

Ａ．立入検査対象選定プロセス

正確性を期すために、C-TPAT 参加者のセキュリティ・プロフィールが検査される。立入検査のために C-TPAT 参加者のセキュリティ・プロフィールが選び出されるその順序はセキュリティリスク・マネージメント原則に基くことになる。立入検査は、輸入量、通常とは異なる状況に係わるセキュリティ、地理的条件による戦略的脅威、あるいは情報に関連するその他のリスクに基づくこともある。これらとは別に、通常の監督プログラムとして立入検査が行われることもある。米国税関の現場事務所（field office）が立入検査を実施することはないし、事前通知なしで立入検査が実施されることもない。C-TPAT 参加者は必要とされる関係文書の準備要求と併せて 30 日前に文書で通知される。

Ｂ．パートナーシップ検査チーム

パートナーシップ検査チーム（PVT：Partnership Validation Team）は米国関税庁 Office of Field Operations の係官と C-TPAT 参加企業の担当代表者から構成されるが、その PVT が米国税関の C-TPAT 参加企業の代表者が立入検査を実施する。

PVT の税関側代表者（Representatives）はサプライチェーン・セキュリティ問題に詳しい係官が務める。税関側 PVT メンバーは、効果的な企業サプライチェーン・セキュリティ・プログラムを促進するための企業の担当代表者との協力を支援するため、サプライチェーン・セキュリティ・トレーニングを受ける。米国関税庁本庁が、個々の PVT の税関側の担当代表者を決定する。税関側の PVT 担当代表者は全て米国関税庁 Office of Field Operations の係官である。

米国税関 PVT のチーム・リーダー（米国関税庁本庁が任命する）が、同チームによる以下についての審査に責任を負う。すなわち、企業のセキュリティ・プロフィール、当該企業によって提出されたその他セキュリティ関連情報、検査の重点項目を決定するために他のソースから取られた検索可能な情報・データ。これらは、立入検査が確実に効果的で限られた期間内で実施されるようにするのに役立つ。

Ｃ．立入検査の実施場所

検査(Validation)は C-TPAT 参加者のサプライチェーン・セキュリティ・プロフィールについて立入（on-site）で行なう。実際に立入る所は、C-TPAT 検査チームが審査する C-TPAT 参加企業のプロフィールの内容に応じて異なる可能性がある。

通常、C-TPAT 参加企業の国内施設（facility）あるいは事務所（corporate office）において企業担当者によるブリーフィングから開始される。C-TPAT 参加者の国内あるいは海外のサプライチェーンを検査するために追加的なデータまたは情報が求められる場合には、PVT リーダーは、米国関税庁本庁の C-TPAT 担当ディレクターに対して出張許可を申請することになる。

Ｄ．立入検査手続き

米国関税庁本庁からの指示に基き、PVT チームリーダーは、企業に文書で予定された立入検査を通知する。通知は検査開始の少なくとも 30 日前に発行され、必要とされる場合には資料あるいは文書の準備も併せて請求される。また PVT チームリーダーは、検査対象の企業の直接連絡窓口担当者を決めるよう当該企業に連絡する。

個々の立入検査は、当該企業に対してカスタマイズされたものとなり、当該企業のセキュリティ・プロフィールに焦点を当てるものとなる。PVT の税関代表者は立入検査の焦点と範囲を決定するため、当該企業の C-TPAT セキュリティ・プロフィール、当該企業から提出された追加情報、関税庁本庁からの指示を検討（Review）する。

立入検査の準備にあたって、（検査対象企業に）関係のある C-TPAT セキュリティ・リコメンデーションを考慮に入れることもある。リコメンデーションは全て後掲するアタッチメントに掲載されている。これらセキュリティ・リコメンデーションは、参加企業の C-TPAT セキュリティ・プロフィール固有の特色に照らして何が十分であるかを検討するための参照ツールである。リコメンデーションは強制的なものではなく、また効果的なセキュリティ管理業務（プラクティス）に関して全てを網羅しているものではないと理解されている。

前述したように、立入検査を開始するに当って、PVT は（検査）プロセスを議論する目的で企業担当者と面談する。立入検査終了時に、PVT は再び企業担当者と会議を持ち、検査所見を議論する。PVT のメンバーではないか、通常当該企業の税関アカウントマネージャーは、検査プロセスの開始時と終了時に行なわれる企業側のブリーフィングに参加することになる。

Ｅ．検査レポート

検査所見は文書化され、検査チームの最終レポートに含まれるとともに、最終的な編集及び C-TPAT 参加企業と情報共有のために米国関税庁の C-TPAT 担当ディレクターに送付される。理想的には、同レポートは当該 C-TPAT 参加企業に与えられているベネフィットのレベルを確認するか向上させるものである。しかしながら、検査所見に応じて当該企業に与えられている C-TPAT ベネフィットの一部または全ては、脆弱であると確認された点に対応するための是正措置がとられるまで保留されることもあり得る。立入検査の結果から取られる措置に関して、税関の権限は米国関税庁本庁 Border Security and Facilitation、Office of Field Operations の Executive Director にある。

ATTACHMENT　A

序

以下は、立入検査を計画する段階で C-TAPT 検査チームが利用する C-TPAT セキュリティ・リコメンデーションの概略を記したものである。これらリコメンデーションは C-TPAT 参加者にとって強制的なものではないが、参加企業の C-TPAT セキュリティ・プロフィールのキーとなる要素を立入検査前にレビューするのに役立つであろう。したがって、立入検査実施に先立って、検査チームは、参加企業の C-TPAT セキュリティ・プロフィールに照らして、このアタッチメントに掲載されているリコメンデーションの中から相応しいセキュリティ・リコメンデーションをレビューし議論することになろう。これは、検査の範囲を限定し、また当該 C-TPAT 参加企業にあわせて検査をカスタマイズするのに役立つものになるだろう。

輸入者

自社のサプライチェーン全般にわたるセキュリティ手続を強化するための計画を立案し実施すること。C-TPAT のセキュリティ・リコメンデーションに係わる施設、輸送あるいはプロセスに対して輸入者が管理権限を有していない場合には、輸入者は、それぞれに責任を有する企業によるコンプライアンスを確かなものにするために、適切なあらゆる努力を払うことに同意する。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。

手続上のセキュリティ：手続は、サプライチェーンの中に積荷目録に記載されていない物が持ち込まれることがないよう設定されなければならない。セキュリティ管理は、貨物の搬入／撤去についての監督、積荷目録などの書類で裏付けられている貨物及び貨物機器に関連する適切な表示、検量、個数勘定及び文書化、過小／過剰積載の発見と報告、コンテナ・トレーラー・鉄道貨車へのシール検証（Verifying）手続を含まなければならない。貨物の搬入／搬出の動向はモニターされなければならない。サプライチェーンの中で、貴社が管理しているエリアについてのセキュリティ・アセスメントについて抜き打ち検査を実施しなければならない。規則からの逸脱行為あるいは違法行為が発見されるか疑われる場合の税関及びその他関係当局への通知手続も規定されなければならない。

物理的なセキュリティ：すべての建物及び鉄道ヤードは、外部からの不法な侵入に耐えられる素材で建築されなければならない。物理的セキュリティは以下のものを装備しなければならない。すなわち、外周フェンス（Perimeter Fences)、外部及び内部ドア・窓・フェンスへの施錠装置、施設内外に対する十分な照明、倉庫内にある国際貨物、国内貨物、高額貨物、危険物などを安全なケージまたはフェンスなどで分離し表示すること。

アクセス管理：施設および搬送部分への許可されない立ち入りは禁止されなければならない。管理内容は、全ての従業員、訪問者、出入り業者（Vender）に対する明示的な身分証確認（Identification）を行うものでなければならない。手続は無許可及び身分の明らかでない物への誰何を行うものでなければならない。

従業員セキュリティ：企業は、採用スクリーニング、採用予定者へのインタヴューを実施し、定期的な従業員のバックグラウンド・チェック、履歴書等内容の検証を行わなければならない。

教育とトレーニング：セキュリティ意識向上プログラムは、内部共謀の察知、貨物安全性の維持、不許可アクセスへの対応等を育むものでなければならない。こうした教育プログラムは、セキュリティ管理における従業員の主体的な参加についてインセンティブを提供するものでなければならない。

積荷目録手続き：企業は、積荷目録が、完全で、判読し易く、正確でタイムリーに関税局へ提出されることを確実にしなければならない。

貨物室（Conveyance）セキュリティ：貨物運搬設備は、許可されない人員及び資材の持ち込みから保護されるように保全されなければならない。セキュリティは、容易にアクセスできる全てのエリアに対する物理的検査、内部と外部を隔てるコンパートメント／パネルの確保、許可されない人間の立ち入り、目録に記載されていない資材の、いたずらされた兆候等が発見された場合の対応手続を含むものでなければならない。

ブローカー

自社のサプライチェーン全般にわたるセキュリティ手続を強化するための計画を立案し実施すること。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。

手続上のセキュリティ：規則からの逸脱行為あるいは違法行為が発見されるか疑われる場合にはいつでも、税関及びその他関係当局への通知しなければならない。

文書管理プロセス：ブローカーは、輸出／輸入者、フレイト・フォワーダー等によって提出されるもので貨物の通関に提出される全ての情報が、明瞭で、差し替えられたり、失われたり、虚偽の情報が入り込むことのないよう最善の努力をしなければならない。文書管理は以下に対する
手続きを含まなければならない。

- 受領した情報の正確さを維持すること。かかる情報とは、通関される貨物に関する、荷主及び荷受人の名前と住所、最初及び 2 番目に通知されるべき人／企業、貨物明細、重量、数量、数量単位（ボックス、カートン等）
- 貨物の過小／過剰を記録、報告、及び／或いは検査すること
- コンピュータへのアクセスと情報に対する保護

従業員セキュリティ：連邦、州、地方政府の法律・規則に沿って、企業は、採用予定者をスクリーニングし履歴書等内容の検証を行う内部手続きを確立しなければならない。このような内部プロセスは、定期的な従業員のバックグラウンド・チェック、その他個別従業員が果たす業務内容に応じた検証を含む事もありうる。

教育とトレーニング：セキュリティ意識向上プログラムは、規則からの逸脱行為あるいは違法行為が発見されるか疑われる場合にはいつでも、税関及びその他関係当局への通知しを行なうということを含まなければならない。これらプログラムは次のようなものを含む。

- セキュリティ管理における従業員の主体的な参加について認識させる
- 不正文書及びコンピュータ・セキュリティ管理に関するトレーニング

製造者

セキュリティ手続を強化するための計画を立案し実施すること。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。企業は下記に対応するセキュリティ手続プランを書面で整備しなければならない。

物理的なセキュリティ：すべての建物及び鉄道ヤードは、外部からの不法な侵入に耐えられる素材で建築されなければならない。物理的セキュリティは以下のものを装備しなければならない。

- 外部及び内部ドア・窓・ゲート・フェンスへの適切な施錠装置。
- 倉庫内にある国際貨物、国内貨物、高額貨物、危険物などを安全なケージまたはフェンスなどで分離し表示すること。
- 駐車エリアを含め、施設内外に対する十分な照明。
- 個人用自動車駐車エリアを、積み出し・積み下ろしドック及び貨物エリアから分離すること。
- セキュリティ担当者あるいは地域の警察と連絡が取れるよう、内部／外部通信システムを整備すること。

アクセス管理：積み出し・積み下ろしドック、貨物エリアへの許可されない立ち入りは禁止されなければならない。管理は次のものを含まなければならない。

- 全ての従業員、訪問者、出入り業者（Vender）に対する明示的な身分証確認（Identification）を行う。
- 無許可及び身分の明らかでない者への誰何を行うための手続。

手続上のセキュリティ：搬入／搬出貨物の取扱方法は、いかなる合法あるいは非合法物質の侵入、差し替え、逸失を防ぐものでなければならず、次のものを含まなければならない。

- 貨物の持ち込み及び撤去についての監督するセキュリティ担当者を置くこと。
- 貨物に対する、適切なマーキング、検量（重量と個数）、裏付け文書。
- コンテナ・トレーラー・鉄道貨車へのシール検証（Verifying）手続。
- 過小／過剰積載の発見と報告。
- 搬入／搬出貨物の動きに対するタイムリーなトラッキング手続。
- 許可されないアクセスを阻止するため、空のコンテナおよび積載コンテナの適切な蔵置。
- 規則からの逸脱行為あるいは違法行為が発見されるか疑われる場合の税関及びその他関係当局への通知手続。

従業員セキュリティ：企業は、採用スクリーニング、採用予定者へのインタヴューを実施し、定期的な従業員のバックグラウンド・チェック、履歴書等内容の検証を行わなければ

ならない。

教育とトレーニング：セキュリティ意識向上プログラムは、内部共謀の察知、貨物の完全性（Integrity）の維持、不許可アクセスへの対応等を育むものでなければならない。こした教育プログラムは、セキュリティ管理における従業員の主体的な参加を促進するものでなければならない。

倉庫管理者（Warehouses）

セキュリティ手続を強化するための計画を立案し実施すること。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。本ガイダンスで定義されるウエアハウスとは保税貨物及び非保税貨物の両方について、蔵置及び留め置く（Stage）ために用いられる施設を言う。企業は次に対応するための文書化されたセキュリティ手続体制を整備しなければならない。

物理的なセキュリティ：すべての建物及び鉄道ヤードは、外部からの不法な侵入に耐えられる素材で建築されなければならない。物理的セキュリティは以下のものを装備しなければならない。

- 外部及び内部ドア・窓・ゲート・フェンスへの適切な施錠装置。
- 駐車エリアを含め、施設内外に対する十分な照明。
- 倉庫内にある国際貨物、国内貨物、高額貨物、危険物などを安全なケージまたはフェンスなどで分離し表示すること。
- 個人用自動車駐車エリアを、積み出し・積み下ろしドック及び貨物エリアから分離すること。
- セキュリティ担当者あるいは地域の警察と連絡が取れるよう、内部／外部通信システムを整備すること。

アクセス管理：施設への許可されない立ち入りは禁止されなければならない。管理は次のものを含まなければならない。

- 全ての従業員、訪問者、出入り業者（Vender）に対する明示的な身分証確認（Identification）を行う。
- 無許可及び身分の明らかでない者への誰何を行うための手続。

手続上のセキュリティ：積荷目録にない物質がウエアハウス内に持ち込まれるのを防ぐよう手続は整備されなければならない。セキュリティ管理は次のものを含まなければならない。

- 貨物の持ち込み及び撤去を監督するセキュリティ担当者を置くこと。
- 貨物に対する、適切なマーキング、検量（重量と個数）、積荷目録の内容を証明できる貨物／貨物機器の文書化。
- コンテナ・トレーラー・鉄道貨車へのシール検証（Verifying）手続。
- 過小／過剰積載の発見と報告。
- 規則からの逸脱行為あるいは違法行為が発見されるか疑われる場合の税関及びその他関係当局への通報手続。
- 許可されないアクセスを阻止するため、空のコンテナおよび積載コンテナの適切な蔵置。

従業員セキュリティ：企業は、採用スクリーニング、採用予定者へのインタヴューを実施し、定期的な従業員のバックグラウンド・チェック、履歴書等内容の検証を行わなければならない。

教育とトレーニング：セキュリティ意識向上プログラムは、内部共謀の察知、貨物完全性（Integrity）の維持、不許可アクセスへの対応等を育むものでなければならない。こした教育プログラムは、セキュリティ管理における従業員の主体的な参加を促進するものでなければならない。

航空会社（Air　Carrier）

セキュリティ手続を強化するための計画を立案し実施すること。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。

貨物室セキュリティ：航空機の完全性（Integrity）が、許可されていない人間及び物質の侵入を防ぐよう維持されなければならない。貨物室セキュリティは、容易にアクセスできる全てのエリアに対する物理的検査、内部と外部を隔てるコンパートメント／パネルの安全確保、許可されない人間の立ち入り、目録に記載されていない資材の持ち込み、いたずらされた兆候等が発見された場合の対応手続を含むものでなければならない。

アクセス管理：航空機への許可されない立ち入りは禁止されなければならない。管理内容は、全ての従業員、訪問者、出入り業者（Vender）に対する明示的な身分証確認（Identification)、記録、行動確認（Tracking）を行い、無許可及び身分の明らかでない者への誰何を行うものでなければならない。

手続上のセキュリティ：手続は、積荷目録に記載されていない物が航空機内に持ち込まれることがないよう整備されなければならない。セキュリティ管理は、全ての荷物に対する一貫したセキュリティを提供する荷物確認システム（positive baggage identification system）だけでなく、貨物、搭乗員、国際旅客についての完全で正確な事前リストを含まなければならない。全ての貨物／貨物機器は、セキュリティ担当者の監督の下で、適切に表示され、検量（重量、個数）され、文書化されなければならない。過小／過剰積載の記録、報告、及び／或いは発見のための手続がなければならない。さらに、規則からの逸脱行為あるいは違法行為が航空会社によって発見あるいは疑われる場合の税関及びその他関係当局への通報手続も規定されなければならない。

積荷目録手続き：企業は、積荷目録が、完全で、判読し易く、正確でタイムリーに関税局へ提出されることを確実にしなければならない。

従業員セキュリティ：採用スクリーニング、採用予定者へのインタヴュー、定期的な従業員のバックグラウンド・チェックを行わなければならない。

教育とトレーニング：セキュリティ意識向上プログラムは、内部共謀の察知、貨物及び荷物安全性の維持、不許可アクセスへの対応等を育むものでなければならない。こうした教育プログラムは、セキュリティ管理における従業員の主体的な参加を促進するものでなければならない。

物理的なセキュリティ：キャリアの建物、ウエアハウス及び離発着ランプ施設は、外部か

らの不法な侵入に耐えられる素材で建築されなければならない。物理的セキュリティは、外部及び内部ドア・窓・フェンスへの施錠装置を装備しなければならない。施設内外に対する十分な照明に加え、駐車エリアもその範囲内に取り込んだ外周フェンス（Perimeter Fence）を設置しなければならない。また倉庫内にある国際貨物、国内貨物、高額貨物、危険物などを安全なケージまたはフェンスなどで分離し表示しなければならない。

船社（Sea　Carrier）

セキュリティ手続を強化するための計画を立案し実施すること。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。

貨物室セキュリティ：船体の安全性は、許可されていない人間及び物質の侵入を防ぐよう維持されなければならない。貨物室セキュリティは、容易にアクセスできる全てのエリアに対する物理的検査、内部と外部を隔てるコンパートメント／パネルの安全確保、許可されない人間の立ち入り、目録に記載されていない資材の持ち込み、いたずらされた兆候等が発見された場合の対応手続を含むものでなければならない。

アクセス管理：船体への許可されない立ち入りは禁止されなければならない。管理内容は、全ての従業員、訪問者、出入り業者（Vender）に対する明示的な身分証確認（Identification）、を含むものでなければならない。無許可及び身分の明らかでない者への誰何を行うものでなければならない。

手続上のセキュリティ：手続は、積荷目録に記載されていない物が船体内に持ち込まれることがないよう整備されなければならない。セキュリティ管理は、搭乗員、旅客についての完全で正確な事前リストを提供するものでなければならない。貨物は、指定されたセキュリティ担当者の監督の下で安全が確保された仕方で積み上げ／積み下ろしされなければならず、過小／過剰積載は適切に発見、報告されなければならない。規則からの逸脱行為あるいは違法行為が当該船会社によって発見あるいは疑われる場合の税関及びその他関係当局への通報手続も規定されなければならない。

積荷目録手続き：積荷目録は、関税規則にしたがって、完全で、判読し易く、正確でタイムリーに申告されなければならない。

従業員セキュリティ：採用スクリーニング、採用予定者へのインタヴュー、履歴書等内容の検証を実施し、定期的な従業員のバックグラウンド・チェックが行わなければならない。

教育とトレーニング：セキュリティ意識向上プログラムは、内部共謀の察知、貨物及び荷物の完全性の維持、不許可アクセスへの対応等を育むものでなければならない。こうした教育プログラムは、セキュリティ管理における従業員の主体的な参加を促進するものでなければならない。

物理的なセキュリティ：キャリアの建物は、外部からの不法な侵入に耐えられる素材で建築されなければならない。物理的セキュリティは、外周フェンス（Perimeter Fence）、施設内外に対する十分な照明、外部及び内部ドア・窓・フェンスへの施錠装置を装備しなけ

ればならない。

陸運会社（Land Carrier）

セキュリティ手続を強化するための計画を立案し実施すること。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。

貨物室セキュリティ：完全性（Integrity）は、許可されていない人間及び物質の侵入保護されるよう維持されなければならない。貨物室セキュリティは、容易にアクセスできる全てのエリアに対する物理的検査、内部と外部を隔てるコンパートメント／パネルの安全確保、許可されない人間の立ち入り、目録に記載されていない資材の持ち込み、いたずらされた兆候等が発見された場合の対応手続を含むものでなければならない。

物理的なセキュリティ：すべてのキャリアの建物及びレール・ヤードは、外部からの不法な侵入に耐えられる素材で建築されなければならない。物理的セキュリティは、外部及び内部ドア・窓・フェンスへの施錠装置を装備しなければならない。施設内外に対する十分な照明に加え、駐車エリアもその範囲内に取り込んだ外周フェンス（Perimeter Fence）を設置しなければならない。また倉庫内にある国際貨物、国内貨物、高額貨物、危険物などを安全なケージまたはフェンスなどで分離し表示しなければならない。

アクセス管理：施設及び搬送装置への許可されない立ち入りは禁止されなければならない。管理内容は、全ての従業員、訪問者、出入り業者（Vender）に対する明示的な身分証確認（Identification）を行い、無許可及び身分の明らかでない者への誰何を行うものでなければならない。

手続上のセキュリティ：手続は、積荷目録に記載されていない物が貨物室内に持ち込まれることがないよう整備されなければならない。セキュリティ管理は、貨物／貨物機器について、セキュリティ担当者の監督の下で、適切に表示され、検量（重量、個数）され、文書化されなければならない。またコンテナ・トレーラー・鉄道貨車へのシール検証手続（Verifying）が規定されていなければならず、過小／過剰積載の記録、報告、及び／或いは発見のための手続が規程されていなければならない。搬入／搬出貨物の時間通りの動きが追跡されなければならず、さらに、規則からの逸脱行為あるいは違法行為が当該企業によって発見あるいは疑われる場合の税関及びその他関係当局への通報手続も規定されなければならない。

積荷目録手続き：企業は、積荷目録が、完全で、判読し易く、正確でタイムリーに関税局へ提出されることを確実にしなければならない。

従業員セキュリティ：企業は、採用スクリーニング、採用予定者へのインタヴューを実施し、定期的な従業員のバックグラウンド・チェック、履歴書等内容の検証を行わなければ

ならない。

教育とトレーニング：セキュリティ意識向上プログラムは、内部共謀の察知、貨物及び荷物安全性の維持、不許可アクセスへの対応等を育むものでなければならない。こうした教育プログラムは、セキュリティ管理における従業員の主体的な参加についてインセンティブを提供するものでなければならない。

航空貨物混載業者／海上輸送仲介業者、及び NVOCC

AIR FREIGHT CONSOLIDATORS/
OCEAN TRANSPOTATION INTERMEDIARIES, AND NVOCC

自社のサプライチェーン全般にわたるセキュリティ手続を強化するための計画を立案し実施すること。以下は、輸入者に対するセキュリティーリコメンデーションであるが、個々の企業の規模や構造に応じてケース・バイ・ケースで対応されるべき一般的なリコメンデーションであり、全てに適用できるものではない。

手続上のセキュリティ：規則からの逸脱行為あるいは違法行為が発見されるか疑われる場合にはいつでも、税関及びその他関係当局への通知しなければならない。

文書管理プロセス：混載業者は、輸出／輸入者、フレイト・フォワーダー等によって提出されるもので貨物の通関に提出される全ての情報が、明瞭で、差し替えられたり、失われたり、虚偽の情報が入り込むことのないよう最善の努力をしなければならない。文書管理は以下に対する
手続きを含まなければならない。

- 受領した情報の正確さを維持すること。かかる情報とは、通関される貨物に関する、荷主及び荷受人の名前と住所、最初及び 2 番目に通知されるべき人／企業、貨物明細、重量、数量、数量単位（ボックス、カートン等）
- 貨物の過小／過剰を記録、報告、及び／或いは検査すること
- 搬入貨物と搬出貨物の動きをトラッキングするための手続
- コンピュータへのアクセスと情報に対する保護

従業員セキュリティ：連邦、州、地方政府の法律・規則に沿って、企業は、採用予定者をスクリーニングし履歴書等内容の検証を行う内部手続きを確立しなければならない。このような内部プロセスは、定期的な従業員のバックグラウンド・チェック、その他個別従業員が果たす業務内容に応じた検証を含む事もありうる。

教育とトレーニング：セキュリティ意識向上プログラムは、規則からの逸脱行為あるいは違法行為が発見されるか疑われる場合にはいつでも、税関及びその他関係当局への通報を行なうことを含むものでなければならない。これは次のようなものを含む。

- セキュリティ管理における従業員の主体的な参加について認識させる
- 不正文書及びコンピュータ・セキュリティ管理に関するトレーニング