最低限セキュリティ基準 – 外国製造業者

２０２０年１月

注意: 基準 ID 番号は連続していないこともあります。リストに挙がっていない ID 番号は外国製造業者には適用されません。

第一の焦点分野: 企業のセキュリティ

1. **セキュリティのビジョンと責任** – CTPAT 参加企業のサプライチェーン・セキュリティプログラムが効果的となり、そうあり続けるためには、企業の幹部の支持がなければなりません。セキュリティを企業文化の欠かせることのできない一部として浸透させ、それが企業全体の優先課題であることを保証することは、主に企業の指導陣の責任です。

ID	基準	実施ガイダンス	必須 / 勧告
1.1	セキュリティの文化を促進する際、CTPAT 参加企業は、支持声明を通じて、サプライチェーンのセキュリティと CTPAT プログラムへのコミットメントを示す必要があります。 声明は、会社の上級役員によって署名され、会社の適切な場所に表示される必要があります。	支持声明では、麻薬密売、テロリズム、人の密輸、禁制品売買などの犯罪行為からサプライチェーンを保護することの重要性を強調する必要があります。 声明を支持し、署名する必要がある会社の上級役員には、社長、CEO、総括管理者、あるいはセキュリティ担当責任者が含まれます。 支持声明を表示する場所としては、会社のウェブサイト、会社の重要区域（受付、梱包、倉庫など）のポスターが含まれ、および/または会社のセキュリティセミナーなどの一部にもなります。	勧告

ID	基準	実施ガイダンス	必須 / 勧告
1.2	強力なサプライチェーン・セキュリティプログラムを構築するには、関連する全部門の代表者をその職域超えをするチームに組み込む必要があります。 これら新しいセキュリティ対策は、既存の企業手順に組み込む必要があります。そうすることにより、さらに持続可能な構造が構築され、サプライチェーンのセキュリティは全員の責任であることが強調されます。	サプライチェーン・セキュリティは、従来のセキュリティプログラムよりもはるかに広範囲に及びます。 人事、情報技術、輸出入などの多くの部門で、セキュリティと密接に関係しています。 より伝統的なセキュリティ部門に基づくモデルを使って構築されたサプライチェーン・セキュリティプログラムは、セキュリティ対策を実施する責任が少数の従業員に集中し、そのため主要な人員の損失に影響を受けやすいという理由で、長期的には実行できなくなる可能性があります。	勧告
1.3	サプライチェーン・セキュリティプログラムは、適切な書面による再検討の余地をもたせることで、設計、支援、実行する必要があります。 この再検討の目的は、担当者が自らの責任と、セキュリティプログラムが概要する全セキュリティ手順が設計どおりに実行されることに説明責任を持つシステムが整備されていることを文書化することにあります。 再検討計画は、組織の運用とリスクのレベルの適切な変更に基づいて、必要に応じて更新する必要があります。	CTPAT の目的を再検討する目標は、従業員が企業のセキュリティ手順に従っていることの確認です。再検討プロセスは複雑である必要はありません。参加企業は、サプライチェーン、ビジネスモデル、リスクのレベル、特定の場所/サイト間の変化における自社の役割に基づいて、再検討の範囲とその深さを決定します。 中小企業は、非常に単純な再検討の方法を作成できます。一方、大規模な多国籍複合企業では、より広範なプロセスが必要になるかもしれず、現地の法的要件など様々な要因を考慮する必要があります。大企業の中には、セキュリティ再検討の支援に影響力を行使できる監査担当者をすでに抱えていることもあります。 参加企業は、特定の手順について対象とする小規模な的を絞った再検討の活用を選択できます。検査や封印管理など、サプライチェーンのセキュリティの鍵となる専門分野は、それらの分	必須

ID	基準	実施ガイダンス	必須 / 勧告
		野に固有な再検討を受ける場合もあります。ただし、セキュリティプログラムの全領域が設計どおりに機能していることを確認するために、全体的な再検討を定期的に実施することは有用です。参加企業が年次再検討の一環としてすでに再検討を実施している場合、そのプロセスはこの基準を満たすために十分です。 高リスクのサプライチェーン（リスク評価によって決定）を持つ参加企業の場合、シミュレーション・卓上演習を再検討プログラムに含めて、実際のセキュリティ事件が発生した場合の対応方法を担当者に確実に知らせることができます。	
1.4	企業の CTPAT への連絡窓口（POC）になる担当者は、CTPAT プログラムの要件についての知識を必要とします。これらの担当者は、監査の進捗状況や結果、セキュリティ関連の演習、CTPAT 検証など、プログラムに関連する問題について定期的に上級管理職に最新情報を提供する必要があります。	CTPAT は、指定された POC が、自社のサプライチェーン・セキュリティ専門家に関与し、対応する積極的な人物であることを期待しています。 参加企業は、CTPAT ポータルに連絡窓口としてリストすることにより、この機能の支援を助けうる追加の人物を特定できます。	必須

2. リスク評価 – サプライチェーンを標的とするテロリスト・グループおよび犯罪組織の継続的な脅威は、これらの進化しつつある脅威に対する既存かつ潜在的な曝露を参加企業が評価することの必要性を強調しています。CTPAT は、企業が多数のビジネスパートナーと共に多くのサプライチェーンを有している場合には、それらのサプライチェーンを保護する上で

もっと複雑な状況に直面すること、を認識しています。企業が多数のサプライチェーンを有する場合、よりリスクの高い地理区域/サプライチェーンに焦点を当てるべきです。

サプライチェーン内のリスクを判断する際、参加企業はビジネスモデル、供給業者の地理的位置、特定のサプライチェーンに固有である他の側面など、さまざまな要因を考慮する必要があります。

重要定義: リスク –脅威、脆弱性、および結果を包括する望ましくない出来事による潜在的な損害の尺度。 リスクのレベルを決定するのは、脅威が発生する可能性がどれだけあるかです。 発生の可能性が高いと、通常、リスクのレベルが高くなります。 リスクをなくすことはできませんが、リスクを管理することで低減することができ、脆弱性や事業への全体的な影響を低減します。

ID	基準	実施ガイダンス	必須 / 勧告
2.1	CTPAT 参加企業は、自社のサプライチェーンにおけるリスク量の判定を実施し、文書化する必要があります。 CTPAT 参加企業は、全体的なリスク評価（RA）を実施して、セキュリティの脆弱性が存在する可能性がある場所を特定する必要があります。 RA は、脅威を特定し、リスクを評価し、脆弱性を低減するための持続可能な手段を取り入れる必要があります。 参加企業は、サプライチェーンに	全体的なリスク評価（RA）は、二つの重要な部分から構成されています。 第一の部分は、CTPAT の最低限セキュリティ基準の遵守を検証するために自社が管理する施設内の参加企業のサプライチェーン・セキュリティ慣行、手順、および方針の自己評価と、リスクをどう管理しているかについての管理層による全体的な再検討です。 RA の第二の部分は、国際的なリスク評価です。 RA のこの部分には、参加企業のビジネスモデルとサプライチェーンにおける役割に基づいた地理的脅威の特定が含まれます。 参加企業のサプライチェーンのセキュリティに対する各脅威の影響を検討する場合、その参加企業はリスクのレベルを評価・区別する方法を必要とします。 単純な方法は、リスクのレベルを低、中、高に割り当てることです。 CTPAT は、参加企業の全体的なリスク評価の国際的なリスク評価部分を実施する支援として、5 段階のリスク評価ガイドを作成しましたが、それは、米国税関国境取締局の Web サ	必須

ID	基準	実施ガイダンス	必須 / 勧告
	おける参加企業の役割に固有のCTPAT 要件を考慮する必要があります。	イト https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf で閲覧できます。 広範なサプライチェーンを有する参加企業の場合、リスクの高い領域に主に焦点を当てることが予想されます。	
2.2	リスク評価の国際的な部分では、原産地から輸入業者の物流センターまでのサプライチェーン全体の参加企業による貨物の移動の文書化や地図作成化の必要があります。 地図作成には、商品の輸出/移動に直接・間接に関与する全ビジネスパートナーを含める必要があります。 該当する場合、地図作成には、貨物が輸送施設/貨物ハブに出入りする方法を文書化し、貨物がこれらの場所のいずれかで長期間「休止」しているかどうかを記録する必要があります。 貨物は、その旅程の次の区間への移動を待っている「休止中」のときに一層脆弱となります。	サプライチェーンの地図作成のプロセスを作る場合、リスクの高い領域を最初に考慮します。 すべての貨物の移動を文書化する場合、参加企業は、輸出入書類のみを処理する通関業者や貨物を直接扱わないが運用管理を行う非船舶運航の一般運送業者（NVOCC）あるいは第三者ロジスティクス提供業者（3PL）などのその他の業者を含めて、該当する全関係者を考慮する必要があります。 輸送の一部が下請けされている場合は、間接的な関係者の層が増えるほどリスクも大きくなるため、この点も考慮したほうがいいかもしれません。 地図作成の演習では、サプライチェーンの仕組みをさらに詳しく調べます。 リスクを特定するだけでなく、サプライチェーンが非効率な領域を見つけるのにも役立ち、その結果、製品を受け取るためのコストや準備期間を削減する方法を見つけることもできます。	勧告

ID	基準	実施ガイダンス	必須 / 勧告
2.3	リスク評価は、年次再検討する必要がありますが、リスク要因が必要とする場合にはそれより頻繁に行う必要があります。	1 年に 1 回よりも頻繁にリスク評価を再検討する必要がある状況としては、特定国からの脅威レベルの高まり、警戒が強化される期間、セキュリティ違反やその事件後、ビジネスパートナーの変更、および/または合併や買収などによる企業構造や所有権の変更が含まれます。	必須
2.4	CTPAT 参加企業は、危機管理、事業継続性、セキュリティ回復計画、および事業再開に対処する手順を文書化する必要があります。	危機には、サイバー攻撃、火災、あるいは武装集団による運送業者の運転手の乗っ取りなどによる貿易データの移動の中断が含まれます。 リスクに基づいて、かつ参加企業が事業を行っている場所や出所に基づいて、緊急時対応計画には、追加のセキュリティ通知・支援、破壊・盗難されたものを回復し、通常の動作状態に戻す方法が含まれうるのです。	勧告

3. ビジネスパートナー – CTPAT 参加企業は、国内外のさまざまなビジネスパートナーと連携しています。貨物および/または輸出入書類を直接扱うビジネスパートナーについては、参加企業はこれらビジネスパートナーが国際的サプライチェーン全体で商品の保護に適切なセキュリティ対策を講じていることを確認することが重要です。ビジネスパートナーが特定の機能を下請けに委託する場合、その均衡状態は一層複雑になり、サプライチェーンのリスク分析を行う際にそれを考慮しなければなりません。

重要定義: ビジネスパートナー –ビジネスパートナーとは、CTPAT 参加企業のサプライチェーンを介して米国に輸入・輸出される物品の保管のセキュリティに影響を与える可能性のある個人や企業です。 ビジネスパートナーは、企業の国際的なサプライチェーン内のニーズを満たすためのサービス業務を提供する任意の関係者です。 これらの役割には、CTPAT 輸入者・輸出者である参加企業のために、あるいはそれに代わって、貨物の購入、文書の準備、円滑化、取り扱い、保管、および/または移動に関与するすべての関係者（直接および間接的）が含まれます。 間接パートナーの 2 つの例は、エージェント/ロジスティクス提供業者が手配する下請け業者と海外の統合倉庫です。

ID	基準	実施ガイダンス	必須 / 勧告
3.1	CTPAT 参加企業は、新しいビジネスパートナーを審査し、現在のパートナーを監視するため、書面化されたリスク基盤プロセスを持っている必要があります。 参加企業がこのプロセスに含めるべき要素は、マネーロンダリングとテロ資金に関連する活動の調査です。 このプロセスの支援には、取引ベースのマネーロンダリングおよびテロ資金調達活動に関する CTPAT の警告指標を参照してください。	以下は、会社が合法かどうかの判断に役立つ審査要素の数例です。 •会社の所在地住所とその住所にいた期間を確認する。 •会社と社主の両方からインターネット上で調査を実施する。 •ビジネス照会の確認。 •クレジットレポートの要求。 審査が必要なビジネスパートナーの例は、製造業者、製品供給業者、関連納入業者/サービス提供業者、輸送/物流提供業者などの直接ビジネスパートナーです。 会社のサプライチェーンに直接関連する、および/または機微情報/機器を処理する納入業者/サービス提供業者も、審査対象リストに含まれます。 これには、ブローカーや契約 IT 提供業者が含まれます。 審査の詳細度は、サプライチェーンのリスクのレベルに依ります。	必須
3.4	ビジネスパートナーの審査プロセスでは、パートナーが CTPAT 参加企業であるか、米国（あるいは承認された MRA）との相互承認協定（MRA）を持つ承認された認定事業者（AEO）プログラムの参加企業であるか、を考慮する必要があります。 CTPAT あるいは承認された AEO のいずれかの認証は、ビジネスパートナーのプログラム要件を満たしていることの許容可能な証拠であり、参加企業は認証の証拠を取得し、これらのビジネスパートナーが引き続き認証を維持していることを確認する必要があります。	ビジネスパートナーの CTPAT 認定は、CTPAT ポータルの地位検証インターフェイスシステムを介して確認できます。 ビジネスパートナーの認定が、米国との MRA を結ぶ外国の AEO プログラムからのものである場合、外国の AEO 認定にはセキュリティ要素が含まれます。 参加企業は、その税関の AEO の氏名がリストされている外国の税関当局のウェブサイトにアクセスするか、ビジネスパートナーに直接認証を要求できます。	必須

ID	基準	実施ガイダンス	必須 / 勧告
		米国の MRA には現在、ニュージーランド、カナダ、ヨルダン、日本、韓国、欧州連合（28 の加盟国）、台湾、イスラエル、メキシコ、シンガポール、ドミニカ共和国、ペルーが含まれます。	
3.5	CTPAT 参加企業がそのサプライチェーンの要素を外部委託や契約をする場合、その参加企業は（訪問、アンケートなどを介して）デューデリジェンスを行使して、これらのビジネスパートナーが CTPAT の最低限セキュリティ基準（MSC）を満たすかそれ以上のセキュリティ対策を講じていることを確認の必要があります。	輸入業者と輸出業者は、サプライチェーン活動の大部分を外部委託する傾向があります。輸入業者（および一部の輸出業者）は、これらの取引の当事者であり、通常はビジネスパートナーに対する影響力があり、保証されている通りに、サプライチェーン全体にセキュリティ対策を実施する必要があります。 CTPAT あるいは承認された MRA の参加企業ではないビジネスパートナーの場合、CTPAT 参加企業は（行使できる影響力をもつ場合）これらのビジネスパートナーがプログラムの該当するセキュリティ基準を満たしていることを確認するためにデューデリジェンスを行使します。 セキュリティ要件の遵守確認のために、輸入業者はビジネスパートナーのセキュリティ評価を実施します。ビジネスパートナーのセキュリティプログラムに関して収集される情報量を決定するプロセスは、参加企業のリスク評価に基づくもので、サプライチェーンが多数ある場合は、リスクの高い地域が優先されます。 ビジネスパートナーが MSC を遵守しているかどうかの判断には、いくつかの方法があります。リスクに基づいて、会社は施設で現場監査を実施するか、請負業者/サービス提供業者を雇って現場監査を実施するか、セキュリティアンケートを使用するかします。セキュリティアンケートを使用する場合、リスクのレベルによっ	必須

ID	基準	実施ガイダンス	必須 / 勧告
		て、収集する必要のある詳細情報や証拠量が決まります。リスクの高い地域に所在する企業には、詳細情報が必要となる場合があります。参加企業がセキュリティアンケートをビジネスパートナーに送信する場合は、次の項目を要求することを検討してください。 •記入した人物の氏名と役職。 •完了日。 •文書の記入完了を行った人物の署名。 •*アンケートの正確性を証明するための、会社の上級役員、セキュリティ監督者、あるいは承認された会社の代表者の署名。 •遵守状況を判断するのに十分な詳細を応答で提供。 •リスクに基づき、地元のセキュリティプロトコルで許可されている場合は、写真の証拠、方針/手順のコピー、および国際交通検査のチェックリストやガードログなどの記入済み用紙のコピーを含める。 *署名は電子署名でも構いません。署名の取得/検証が困難な場合、回答者は電子メールでアンケートの有効性を証明し、回答と裏付けとなる証拠が監督者/管理者によって承認されたことを証明できます（氏名と役職が必要です）。	

ID	基準	実施ガイダンス	必須 / 勧告
3.6	ビジネスパートナーのセキュリティ評価中に弱点が確認された場合は、できるだけ早く対処し、タイムリーに修正を行う必要があります。 参加企業は、証拠書類によって欠陥が軽減されたことを確認する必要があります。	CTPAT は、何が修正に必要かに応じて、修正を行うためのさまざまなタイムラインがあることを認識しています。 通常、物理的な機器の設置は手順の変更よりも時間がかかりますが、セキュリティのギャップは発見時にすぐ対処する必要があります。 例えば、問題が破損したフェンスの交換である場合、新しいフェンスを購入するプロセスはすぐに開始の必要があり（欠陥への対処）、新しいフェンスの取付け（修正措置）も可能な限り早く実行する必要があります。 関連リスクのレベルと見つかった脆弱性の重要性に基づいて、問題の中には早急な対応が必要なものもあります。例えば、コンテナのセキュリティを危険にさらす可能性のある欠陥の場合は、できるだけ早く対処する必要があります。 文書証拠の例には、追加の警備員契約書のコピー、新しく設置された防犯カメラや侵入警報の写真、検査チェックリストのコピーなどが含まれます。	必須

ID	基準	実施ガイダンス	必須 / 勧告
3.7	ビジネスパートナーが CTPAT のセキュリティ基準の遵守継続を保証するために、参加企業はビジネスパートナーのセキュリティ評価を定期的に、あるいは状況/リスクに応じて更新する必要があります。	ビジネスパートナーのセキュリティ評価を定期的に確認することは、強力なセキュリティプログラムが適切に機能していることを確認するために重要です。参加企業がビジネスパートナーのセキュリティプログラムの評価の更新を一度も要求しない場合、参加企業はかつて有効だったプログラムがもはや効果的でなくなったことが分かりません。そのため、参加企業のサプライチェーンを危険にさらすことになります。 パートナーのセキュリティ評価の再検討を行う頻度の決定は、参加企業のリスク評価プロセスに基づいています。高リスクのサプライチェーンは、低リスクのサプライチェーンよりも頻繁に再検討されることが予想されます。参加企業が直接訪問することでビジネスパートナーのセキュリティを評価している場合、必要な他の種類の訪問を活用することを検討できます。たとえば、品質管理を試験する相互訓練担当者がセキュリティ管理も実施するといった例があります。 自己評価をより頻繁に更新する必要がある状況には、原産国の脅威レベルの増加、原産地の変更、新しい重要なビジネスパートナー（実際に貨物を処理、施設の保安を提供する企業など）が含まれます。	勧告

ID	基準	実施ガイダンス	必須 / 勧告
3.8	米国への到着貨物については、参加企業が別の高速道路運送業者に輸送サービスを下請けする場合、その参加企業は CTPAT 認定高速道路運送業者、あるいは書面契約に従ってその企業のために直接働く高速道路運送業者を使う必要があります。 契約は、すべての最低限セキュリティ基準（MSC）要件の順守を規定していなければなりません。	運送業者は、下請け運送業者と運転手のリストを、貨物を引き取り配送する施設に提供する必要があります。 下請業者リストの変更は、すぐに関連パートナーに伝えねばなりません。 サービス提供業者の遵守状況を再検討する場合、参加企業は、下請け会社が実際に荷物を輸送している会社であり、承認なしにさらに下請けに委託していないことを確認する必要があります。 参加企業は、輸送業務の下請けを一段階のみに制限する必要があります。 さらなる下請けが例外的に許可されている場合は、CTPAT 参加企業と荷送人に、荷物輸送がさらに下請けされたことを通知する必要があります。	必須

ID	基準	実施ガイダンス	必須 / 勧告
3.9	CTPAT 参加企業は、最低限、米国に輸入された物品が全面的・部分的に禁止された労働形態、すなわち強制労働、懲役労働、年季奉公、あるいは年季奉公の児童労働によって採掘、生産、製造されたものでないことをどのように保証できるかについて対処する文書化された社会遵守プログラムを保有すべきです。	労働者の作業とサプライチェーンにおける労働者の権利を保護する民間企業の努力は、労働法と基準のより良い理解を促進し、劣悪な労働慣行を低減することができます。さらにこれらの努力は、労働者と雇用主の関係を改善する環境を創り、企業の収益を改善します。 1930 年関税法の第 307 項（1 S 9 U.S.C. § 1307）は、強制労働あるいは年季奉公の児童労働（強制児童労働を含む）によって外国で採掘、生産・製造された物品の全部・一部の輸入を禁止しています。 強制労働とは、国際労働機関の第 29 番協定で、懲罰の脅威にさらされた人に対して強制され、その本人が自発的に提供していない全仕事や業務、と定義されています。 社会遵守プログラムとは、社会的・労働上の課題を対象とする行動規範の要素を最大限に遵守することを保証するべく企業が目指す一連の政策と慣行です。社会遵守とは、環境保護、ならびに従業員の健康、安全、権利、従業員が事業を行っている共同体、およびサプライチェーンに沿った労働者の生活と共同体における責任を企業が取り組んでいる方法を指します。	勧告

4. **サイバーセキュリティ** –現在のデジタル世界では、サイバーセキュリティは、企業の最も貴重な資産である知的財産、顧客情報、財務と貿易データ、従業員規則などを保護するための鍵です。インターネットへの接続が増加するにつれ、企業の情報システムが侵害されるリスクが生じます。この脅威は、あらゆる種類・規模の企業に関係しています。企業の情報技術（IT）とデータを保護する対策は非常に重要であり、リストに挙げられている基準は参加企業のサイバーセキュリティ・プラグラム全般の基盤になります。

重要定義: サイバーセキュリティ –サイバーセキュリティは、コンピュータ、ネットワーク、プログラム、およびデータを意図しないあるいは不正なアクセス、改ざん、もしくは破壊からの保護に焦点を当てた活動やプロセスです。 サイバー関連のリスクを特定、分析、評価、伝達し、コストと便益を考慮して、許容可能なレベルまでそれを受け入れ、回避、転送、あるいは軽減するプロセスです。

情報技術 (IT) – ITには、すべての形式の電子データを作成、処理、保存、保護、および交換するためのコンピュータ、貯蔵、ネットワーク、その他の物理デバイス、インフラ、プロセスが含まれます。

ID	基準	実施ガイダンス	必須 / 勧告
4.1	CTPAT 参加企業は、情報技術（IT）システムを保護するための書面化された包括的なサイバーセキュリティ方針と手順を有する必要があります。 文書化された IT 方針は、最低限、個々のサイバーセキュリティ基準の全てを網羅しなければなりません。	参加企業は、認識されている業界のフレームワーク/標準に基づくサイバーセキュリティプロトコルに従うよう薦めます。 * 国立標準技術研究所（NIST）は、内部・外部の両面からのリスクの管理と低減を助けるべく、既存の標準、ガイドライン、慣行に基づいて自主的なガイダンスとなるサイバーセキュリティの枠組み (https://www.nist.gov/cyberframework)を提供する組織の 1 つです。サイバーセキュリティのリスクを低減するための措置を特定して優先順位を付けるために活用でき、リスクを管理するための方針、事業、および技術的アプローチを整合させるためのツールでもあります。この枠組みは、組織のリスク管理プロセスとサイバーセキュリティプログラムを補完します。また、既存のサイバーセキュリティプログラムを有していない組織は、枠組みを確立するための参照基準としても活用できます。 * NIST は、商務省に属する連邦政府の非規制機関であり、測定基準の推進と維持を行っており、連邦政府の技術標準開発機関です。	必須

ID	基準	実施ガイダンス	必須 / 勧告
4.2	情報技術（IT）システムを一般的なサイバーセキュリティの脅威から守るには、企業はマルウェア（ウイルス、スパイウェア、ワーム、トロイの木馬など）および内部/外部侵入（ファイアウォール）からのソフトウェア/ハードウェアの十分な保護を参加企業のコンピュータシステムに導入しなければなりません。 参加企業は、セキュリティソフトウェアが最新のものであり、セキュリティ最新化を定期的に受信していることを確認する必要があります。 参加企業は、ソーシャルエンジニアリングによる攻撃を防ぐための方針と手順を持たねばなりません。 データ侵害が発生した場合、あるいは別の目に見えない出来事によってデータや機器が失われた場合、手順には IT システムやデータの復旧（あるいは交換）を含めなければなりません。		必須

ID	基準	実施ガイダンス	必須 / 勧告
4.3	ネットワークシステムを使用する CTPAT 参加企業は、IT インフラのセキュリティを定期的にテストしなければなりません。 脆弱性が見つかった場合、可能な限り早く是正措置を実施しなければなりません。	安全なコンピュータネットワークは企業にとって最も重要であり、保護を確認するには定期的なテストを行うことが必要です。これは、脆弱性スキャンを予定に組み込むことで実行できます。警備員が企業で開いているドアや窓をチェックするように、脆弱性スキャン（VS）は、コンピュータの開口部（開いているポートと IP アドレス）、オペレーティングシステム、およびハッカーが会社の IT システムへのアクセスを取得できるソフトウェアを特定します。 VS は、スキャンの結果を既知の脆弱性のデータベースと比較することでこれを行い、企業が実行するための修正レポートを作成します。脆弱性スキャナーには多くの無料版と商用版があります。 テストの頻度は、企業のビジネスモデルやリスクのレベルなど、さまざまな要因によって異なります。例えば、企業は、そのネットワークインフラに変更があるたびに、常にテストを行うべきです。ただし、あらゆる規模の企業でサイバー攻撃が増加しているため、テスト計画を立てる際にはこのことを考慮する必要があります。	必須

ID	基準	実施ガイダンス	必須 / 勧告
4.4	サイバーセキュリティ方針は、参加企業が政府や他のビジネスパートナーとサイバーセキュリティの脅威に関する情報をどのように共有するかについて対処すべきです。	参加企業は、サイバーセキュリティの脅威に関する情報を、サプライチェーン内の政府やビジネスパートナーと共有するように、薦めます。 情報共有は、悪意のあるサイバー活動に関する状況認識を共有するという国土安全保障省の使命の重要部分です。 CTPAT 参加企業は、国家サイバーセキュリティ通信統合センター（NCCIC-- https://www.us-cert.gov/nccic）への参加を希望することもできます。 NCCIC は、公共機関と民間企業のパートナー間で情報を共有して、脆弱性、インシデント、および低減策に関する認識を高めています。 サイバー・産業用制御システムのユーザーは、情報製品、フィード、サービスを無料で購読できます。	勧告
4.5	IT システム/データへの不正アクセス、あるいは内部システムや外部ウェブサイトへの不適切なアクセス、従業員や請負業者によるビジネスデータの改ざん・変更を含む方針と手順の悪用を特定するためのシステムを設定しておく必要があります。 すべての違反者は、適切な懲戒処分の対象となります。		必須
4.6	サイバーセキュリティの方針と手順は、リスクや状況に応じて、毎年、あるいはそれより頻繁に再検討しなければなりません。 再検討後、必要に応じて方針と手順を更新しなければなりません。	毎年 1 回よりも頻繁に方針を更新しなければならない状況の例は、サイバー攻撃です。 攻撃から学んだ教訓を活用すると、参加企業のサイバーセキュリティ方針の強化に役立ちます。	必須

ID	基準	実施ガイダンス	必須 / 勧告
4.7	ユーザーのアクセスは、職務内容や任務に基づいて制限しなければなりません。 極秘システムへのアクセスが職務要件に基づいていることを確認するために、承認されたアクセスを定期的に再検討する必要があります。 従業員の離職時には、コンピュータとネットワークへのアクセスを停止しなければなりません。		必須
4.8	情報技術（IT）システムにアクセスできる個人は、個別に割り当てられたアカウントを使用しなければなりません。 強力なパスワード、パスフレーズ、またはその他の形式の認証の使用を通じて、IT システムへのアクセスを侵入から保護しなければならず、IT システムへのユーザーアクセスを保護しなければなりません。 侵害の証拠がある場合、あるいは侵害への合理的な疑いがある場合は、パスワードやパスフレーズをできるだけ早く変更しなければなりません。	IT システムを侵入から保護するには、認証プロセスを経てユーザーアクセスを保護しなければなりません。複雑なログインパスワードやパスフレーズ、生体認証技術、電子 ID カードは、3 種類の認証プロセスです。複数の手段を使用するプロセスがより好ましいのです。これらは、2 要素認証（2FA）あるいは多要素認証（MFA）と呼ばれます。 MFA は、ログオンプロセス中にユーザーの身元を認証するために、ユーザーが 2 つ以上の証拠（資格情報）を提示する必要があるため、最も安全です。 MFA は、脆弱なパスワードや盗まれた資格情報によって悪用されたネットワーク侵入の閉鎖を支援できます。 MFA は、トークンや物理的特徴の 1 つである生体情報など、ユーザーが持っているものでパスワードやパスフレーズ（本人に既知のもの）を補強するよう個人に付けることにより、これらの攻撃ベクトルの閉鎖を支援できます。	必須

ID	基準	実施ガイダンス	必須 / 勧告
		パスワードを使用する場合は、複雑にする必要があります。米国国立標準技術研究所（NIST）の NIST 特別出版物 800-63B：デジタル ID ガイドラインには、パスワードガイドライン（https://pages.nist.gov/800-63-3/sp800-63b.html）が含まれています。特殊文字を含む単語の代わりに、覚えやすいパスフレーズを長く使用することをお薦めします。これらのより長いパスフレーズ（NIST は最大 64 文字の長さを許可することを推奨しています）は、簡単に記憶される文やフレーズで構成されているため、解読するのがはるかに難しいと考えられています。	
4.9	ユーザーがネットワークに遠隔接続を可能にしている参加企業は、従業員が事務所外にいるときに会社のイントラネットに安全にアクセスできるように、仮想プライベートネットワーク（VPN）などの安全な技術を採用しなければなりません。 さらに、参加企業は、許可を得ていないユーザーからの遠隔アクセスを防ぐように設計された手順を持たなければなりません。	ネットワークへの遠隔アクセスを保護する選択肢は VPN だけではありません。 多要素認証（MFA）もその方法です。 多要素認証の例としては、従業員がネットワークにアクセスするために入力の必要がある動的なセキュリティコードを持つトークンなどです。	必須
4.10	従業員が個人のデバイスを使用して会社の業務を行うことを参加企業が許可している場合、そのような全デバイスは、会社のネットワークに安全にアクセスするための定期的なセキュリティ最新化と方法を含む会社のサイバーセキュリティ方針と手順を遵守しなければなりません。	個人用デバイスには、CD、DVD、USB フラッシュドライブなどの記憶媒体が含まれます。 従業員が自らの媒体を個々のシステムに接続することを許可されている場合、これらのデータ記憶装置は企業のネットワークを使用して伝播するマルウェアに感染する可能性があるため、注意が必要です。	必須

ID	基準	実施ガイダンス	必須 / 勧告
4.11	サイバーセキュリティの方針と手順には、模造品あるいは不適切にライセンスされた技術製品の使用を防止するための対策を含めるべきです。	コンピューターソフトウェアは、それを作成した企業主体が所有する知的財産（IP）です。ソフトウェアを取得する方法に関係なく、製造元・発行元の明示的な許可なしにソフトウェアを導入することは違法です。その許可はほとんどの場合、許可されたソフトウェアのコピーに付随する発行者からのライセンスという形をとります。ライセンスされていないソフトウェアは、更新できないために不具合が生じる可能性が高くなります。コンピュータとその情報を役立たなくするマルウェアを含む傾向があります。ライセンスされていないソフトウェアに対する保証や支援は期待できず、会社は独力で不具合に対処することになります。ライセンスのないソフトウェアには、厳しい民事罰や刑事訴追などの法的結果があります。ソフトウェアの不正コピーは、正当な認可されたソフトウェアのユーザーのコストを増加させ、新しいソフトウェアの研究開発に投資するための資金を削減します。 参加企業は、新しい媒体の購入時にプロダクトキーラベルと信頼性の証明書の保持を要求する方針を持つことを薦めます。 CD、DVD、および USB といった媒体には、真正製品を確実に受け取り、模造から保護するためのホログラフィックセキュリティ機能が含まれています。	勧告
4.12	データは 1 週間に 1 回、あるいは必要に応じてバックアップする必要があります。 全極秘データと全機密データは、暗号化された形式で保存すべきです。	データの損失は組織内の個人にさまざまな影響を与える可能性があるため、バックアップを行うべきです。 本番サーバーや共有サーバーが危険にさらされたりデータが失われたりする場合に備えて、毎日のバックアップを薦めます。 関与する情報の種類によっては、個々のシステムで必要なバックアップの頻度が少なくなる場合もあります。	勧告

ID	基準	実施ガイダンス	必須 / 勧告
		バックアップの保存に使用する媒体は、できればオフサイトの施設に保存すべきです。 データのバックアップに使用されるデバイスは、実稼働作業に使用されるものと同じネットワーク上にあってはなりません。 データをクラウドにバックアップすることは、「オフサイト」施設として受け入れられます。	
4.13	輸入/輸出プロセスに関する極秘情報を含むすべての媒体、ハードウェア、その他の IT 機器は、定期的な在庫点検を通じて確認する必要があります。 廃棄する場合は、国立標準技術研究所（NIST）の媒体のサニタイズに関するガイドラインあるいはその他の適切な業界ガイドラインに従って、適切にサニタイズおよび/または破壊する必要があります。	コンピュータ媒体の種類には、ハードドライブ、外付けドライブ、CD-ROM や CD-R ディスク、DVD、あるいは USB ドライブなどがあります。 国立標準技術研究所（NIST）は、政府のデータ媒体破壊基準を作成しました。 参加企業は、IT 機器と媒体のサニタイズや破壊について、NIST 標準を参照することを薦めます。 媒体のサニタイズ： https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	必須

第二の焦点分野: 輸送のセキュリティ

5. **国際運輸セキュリティの輸送機関と器具** – 密輸計画は多くの場合、国際運輸の輸送機関と輸送器材（IIT）の改変あるいは IIT 内への模造品の秘匿よるものです。この基準カテゴリーは、許可されていない物質や人の導入を可能にする IIT 構造の改ざんやそれらへの不正な立ち入りを防止、検知、および/または阻止することを目的とする保安措置を対象とします。

詰め込み/積み込みの時点で、IIT を検査して適切に封印する手順を導入しておく必要があります。 輸送中あるいは「休止中」の貨物は管理が難しいため、侵入に対してより脆弱です。そのため、封印管理と輸送中の貨物/輸送機関を追跡する方法が重要なセキュリティ基準です。

サプライチェーンの侵害は、輸送プロセス中に最も頻繁に発生します。 したがって、参加企業は、これらの重要な貨物基準がサプライチェーン全体で維持されるよう注意しなければなりません。

重要定義: 国際運輸輸送器材 (IIT) – ITT には、国際貿易における物品の出荷に使用中か今後使用される、コンテナ、平床型貨物自動車、ユニット積載装置（ULD）、リフトバン、貨物バン、輸送タンク、集積貯蔵容器、車輪付き荷台、パレット、当て板、織物用芯材、あるいは到着中の特殊コンテナ（積載済みまたは空のもの）が含まれます。

ID	基準	実施ガイダンス	必須/勧告
5.1	国際運輸の輸送機関と輸送器材（IIT）は、不正なアクセスを防ぐために安全な場所に保管しなければなりません。不正アクセスにより、国際輸送器材の構造が変更されたり、（該当する場合）封印/ドアが侵害されたりする可能性があります。	不正なアクセスを防ぐためには、国際運輸の輸送機関と輸送器材（空および満載状態の両方）の安全な保管が重要です。	必須

ID	基準	実施ガイダンス	必須/勧告
5.2	CTPAT 検査プロセスには、セキュリティ検査と農業検査の両方に関する書面による手順書がなければなりません。	国際運輸の輸送機関・輸送器材の改変を伴う密輸計画が流行っているため、参加企業は、目に見える害虫や深刻な構造欠陥を探すために、国際運輸の輸送機関・輸送器材の検査を実施することが不可欠です。同様に、輸送機関と IIT による害虫汚染の防止は最重要事項であるため、セキュリティ検査プロセスに農業要素が追加されています。 害虫汚染は、目に見える形の動物、昆虫、または他の無脊椎動物（生死を問わず、卵殻や浮遊粘着物の塊を含むライフサイクルのあらゆる段階）、あるいは動物由来の有機物質（血液、骨、毛、肉、分泌物、排泄物など）、生育可能か否かを問わず、植物・植物製品（果物、種子、葉、小枝、根、樹皮を含む）、または真菌を含む他の有機材料、もしくは土壌や水であって、当該製品が国際輸送器材（コンテナ、ユニット積載装置など）内の明示された貨物ではないものとして定義されます。	必須
5.3	CTPAT 参加企業は、以下の体系的な CTPAT セキュリティ・農業検査が実施されていることを確認しなければなりません。これらの検査の要件は、サプライチェーンが陸上基盤（カナダあるいはメキシコ）であるか、海外に起源があるもの（海上と航空モード）であるかによって異なります。詰め込み/梱包の前に、国際運輸の輸送器材（IIT）は空の状態ですべて検査しなければなりません。また、輸送機関は、国境を越えて米国に入国する際にも検査を受けねばなりません。	密輸品を隠すために構造が変更されていないこと、ならびに目に見える農業害虫で汚染されていないことを確認するために、国際運輸の輸送器材（IIT）と輸送機関のセキュリティ検査と農業検査が行われます。 海外のサプライチェーンに期待されることは、詰め込み/梱包の時点で IIT のすべての器材を検査することです。ただし、海上/航空によるサプライチェーンのリスクが高い場合は、海上ターミナルあるいは航空物流施設での輸送機関を含むより一層徹底した検査を含めて、より広範な検査手順	必須

ID	基準	実施ガイダンス	必須/勧告
	海、空、陸の国境（該当する場合）を介した鉄道あるいは複合一貫輸送による CTPAT 輸送の検査要件： 空の状態の全コンテナとユニット積載装置（ULD）で 7 点検査を実施しなければなりません。空の状態の全保冷コンテナと全保冷 ULD について 8 点検査を実施しなければなりません： 1.前壁 2.左側 3.右側 4.床面 5.天井/屋根 6.内部/外部ドア、ドアのロック機構の信頼性を含む 7.外側/車台 8.保冷コンテナのファン・ハウジング 高速道路運送業者を介した陸上国境通過の追加検査要件： 輸送機関および IIT の検査は、輸送機関/ IIT 保管場で実施しなければなりません。 可能であれば、保管場に出入する直後に、積み込み/詰め込みの場所で検査を実施する必要があります。 これらの体系的な検査には、17 点の検査が含まれていなければなりません。	を含める必要があります。通常、陸上の国境通過による貨物輸送には高いレベルのリスクが伴うため、輸送機関と IIT の両方で複数の検査が行われます。 さまざまなモードでの IIT の例として、海上コンテナ、保冷コンテナ/トレーラー、路上トレーラー、平床型トレーラー、タンクコンテナ、鉄道/有蓋車、ホッパー、ユニット積載装置（ULD）などがあります。 CTPAT ポータルの公共ライブラリーのセクションには、セキュリティおよび農業輸送機関/国際運輸の輸送器材の検査に関する訓練用資料が入っています。	

ID	基準	実施ガイダンス	必須/勧告
	トラクター： 1.バンパー/タイヤ/リム 2.ドア、ツールコンパートメント、およびロック機構 3.蓄電池外箱 4.空気吸入エンジン 5.燃料タンク 6.仕切り車室/寝台車 7.フェアリング/屋根 トレーラー： 1. 第５輪部分-ナチュラルコンパートメント/スキッドプレートを確認 2.外観-前面/側面 3.後部-バンパー/ドア 4.前壁 5.左側 6.右側 7.床面 8.天井/屋根 9.内側/外側のドアとロック機構 10.外側/車台		

ID	基準	実施ガイダンス	必須/勧告
5.4	（必要に応じて）国際運輸の輸送機関と輸送器材には、それを取り除く試練に耐えうると合理的に考えられる外部ハードウェアが装備されていなければなりません。 封印器具を取り付ける前に、ドア、ハンドル、ロッド、ハスプ、リベット、ブラケット、コンテナのロック機構のその他の全部品を完全に検査して、改変やハードウェアの不整合を検出しなければなりません。	不正開封の防止が可能な蝶番付きのコンテナ/トレーラーの使用を検討してください。 参加企業は、ドアの蝶番の少なくとも 2 つに保護プレートやピンを設置したり、両側の各々に最低 1 つの蝶番に接着シール/テープを貼ったりすることもできます。	必須
5.5	国際運輸の全輸送機関と空の状態の器材の検査は、チェックリストに記録すべきです。 以下の要素をチェックリストに文書化すべきです。 •コンテナ/トレーラー/国際運輸の器材番号 •検査の日付 •検査の時間 •検査を実施する従業員の名前 •検査された国際輸送器材の特定領域 検査が監督されている場合、監督者もチェックリストに署名すべきです。 記入済みのコンテナ/国際運輸器材の検査票は、出荷書類パケットの一部として含めるべきです。 荷受人は、商品を受け取る前に完全な出荷書類パケットを受け取るべきです。		勧告
5.6	全セキュリティ検査は、アクセスが制御された区域で実行し、可能な場合は CCTV システムを介して監視すべきです。		勧告

ID	基準	実施ガイダンス	必須/勧告
5.7	国際運輸の輸送機関/輸送器材の検査中に目に見える害虫の汚染が見つかった場合、その汚染を除去するために洗浄/掃除を行わねばなりません。 これらの検査要件の遵守を証明するために、書類を 1 年間保管しなければなりません。	発見された汚染物質の種類、それが見つかった場所（輸送機関の場所）、害虫汚染がどのように除去されたかを記録することは、参加企業が将来の害虫汚染を防止するのを助ける有用な措置です。	必須
5.8	リスクに基づいて、管理人員は、輸送スタッフが国際輸送の輸送機関と輸送器材の検査を実施した後、輸送機関の無作為な捜索を実施すべきです。 リスクに応じて頻度を増やしながら、輸送機関の捜索を定期的に行うべきです。予測が可能とならないように、捜索は警告なしに無作為で実行されるべきです。検査は、輸送機関が影響を受けやすい様々な場所で実施すべきです。例えば、トラックへの積み込みが終わった後の運送業者の作業場、米国国境に向かう途中などです。	内部陰謀に対抗するために、輸送機関の監督者による捜索が行われます。 ベストプラクティスとして、監督者は現場試験審査官/輸送機関オペレーターが見つけられるかどうかを判断するために、物品（おもちゃや色付きの箱など）を輸送機関に隠すことができます。 監督者は、セキュリティについて上級管理職に説明責任を負っているセキュリティ管理者、あるいはその他の任命済みの管理者であるかもしれません。	勧告
5.14	CTPAT 参加企業は、輸送提供業者と協力して、輸送機関を出発地から最終仕向地まで追跡すべきです。 データの追跡、報告、共有に関する特定の要件を、サービス提供業者との業務契約の条件に組み込むべきです。		勧告
5.15	荷送人は、運送業者の GPS フリート監視システムにアクセスできるようにして、貨物の動きを追跡できるようにすべきです。		勧告
5.16	米国の国境に近い陸上国境を通過する出荷については、予定外の停車に関して「停車禁止」方針を実施すべきです。	休止時の貨物はリスクのある貨物です。 予定されている停車はこの方針の対象ではありませんが、全体的な追跡と監視手順の中で考慮する必要があります。	勧告

ID	基準	実施ガイダンス	必須/勧告
5.24	リスクの高い地域では、国境検問所に到着する直前に、CTPAT参加企業は、国際運輸の輸送機関/輸送器材に改ざんの兆候がないかどうかを確認する点検のための米国行き貨物の「最後のチャンス」検証プロセスを組み込むべきであり、輸送機関の目視検査と VVTT 封印検証プロセスを含めるべきです。 適切に訓練された個人が検査を実施すべきです。 V –封印およびコンテナのロック機構を目視し、それらが正常であることを確認。 V –正確さを期するために、出荷書類に照らして封印番号を確認。 T –封印を引っ張り、適切に取り付けられていることを確認。 T –ボルトシールをねじり回し、構成部品のねじが緩んだり、互いに分離したり、封印の一部が緩んだりしないようにする。		勧告
5.29	出荷や輸送機関のセキュリティに対する信頼に値する（または検知された）脅威が発見された場合、参加企業は、影響を受ける可能性のあるサプライチェーン内のビジネスパートナーと法執行機関に、必要に応じて（できるだけ早く）警告しなければなりません。		必須

6. 封印のセキュリティ –トレーラーとコンテナの封印はその継続的な完全性を含めて、安全なサプライチェーンの重要要素であり続けています。封印セキュリティとは、この全ての面に対処する書面の包括封印方針を保持し、CTPAT 要件に準拠する正しい封印を使用し、IIT に封印を適切に配置し、封印が適切に添付されたことを検証すること、を含めています。

ID	基準	実施ガイダンス	必須/勧告
6.1	CTPAT 参加企業は、施設内と輸送中に封印が発行・管理される方法を説明する詳細な文書化された高セキュリティ封印手順を有する必要があります。この手順書には、出来事の文書化、パートナーへの通信プロトコル、インシデントの捜査を含めて、封印が変更、改ざんされ、あるいは封印番号が不正な場合に実施する手順を含めていなければなりません。調査の結果は文書化し、是正措置は可能な限り迅速に実施しなければなりません。 これらの書面による手順は、簡単にアクセスできるように、現場の運用レベルで維持しなければなりません。手順は最低年 1 回再検討し、必要に応じて更新しなければなりません。 書面による封印管理には、次の要素を含める必要があります。 **封印へのアクセスの制御：** •封印の管理は許可された人員だけに制限。 •安全な保管。 **在庫点検、配布、追跡（封印ログ）：** •新しい封印の受領を記録。 •ログに記録された封印の発行。		必須

ID	基準	実施ガイダンス	必須/勧告
	•ログにより封印を追跡。 •訓練を受け、許可された担当者のみが、国際運輸の輸送器材（IIT）に封印を貼ることができる。 **輸送中の封印の制御：** •封印された IIT を回収する時（あるいは停車した後）、封印が改ざんされていないことを確認。 •封印番号が出荷書類の記載と一致することを確認。 **輸送中に破損した封印：** •積載物を調べる場合は、交換用の封印番号を記録。 •運転手は、封印が破られた場合、直ちに派遣担当に通知し、誰が封印を破ったかを示し、新しい封印番号を受けとらねばならない。 •運送業者は、封印の変更と交換用封印の番号を直ちに荷送人、仲介業者、輸入者に通知しなければならない。 •荷送人は、封印ログに交換用の封印番号を記録しなければならない。 **封印の不一致：** •捜査を助けるために、変更・改ざんされた封印を保持。 •不一致を調査。是正措置によるフォローアップ（必要な場合）。 •必要に応じて、侵害された封印を CBP および適切な外国政府に報告し、調査を支援する。		

ID	基準	実施ガイダンス	必須/勧告
6.2	封印できる CTPAT 全貨物は、責任者（荷送人・荷送人に代わって行動する荷主）による荷積み/詰め込み/梱包の直後に、国際標準化機構（ISO）の最新の高セキュリティ封印 17712 標準に適合するかそれ以上の高セキュリティ封印で安全確保しなければなりません。 認定ケーブルとボルトシールの両方が許容されます。 使用する全封印は、CTPAT 参加企業の貨物を米国との間で輸送している国際運輸の輸送器材に安全かつ適切に添付されなければなりません。	使用する高セキュリティ封印は、右側のドアハンドルの代わりに、可能な場合は安全なカムの位置に配置しなければなりません。 封印は、コンテナ右ドアの最も中央の垂直な棒の下部に配置しなければなりません。 あるいは安全なカム位置が利用できない場合は、コンテナ右ドアの左側の最も中央のロックハンドルに封印を配置できます。 ボルトシールを使用している場合、ボルトシールは円筒部か挿入部を上向きにして、円筒部を掛け金の上に配置することを薦めます。	必須
6.5	（封印の目録を維持する）CTPAT 参加企業は、使用する高セキュリティ封印が最新の ISO 17712 標準を満たしているか、それを超えていることを文書化できなければなりません。	遵守ができていると容認できる証拠は、ISO の高セキュリティ封印規格への準拠を示す実験室試験証明書のコピーです。 CTPAT 参加企業は、購入する封印の改ざんを示す機能を理解している必要があります。	必須
6.6	参加企業が封印の目録を保持している場合、会社の管理者・セキュリティ監督者は、保管された封印の定期的な目録点検およびシール目録ログと出荷書類を照合し一致確認を含めて封印監査を実施しなければなりません。 全監査は文書化しなければなりません。 全体的な封印監査プロセスの一環として、ドック監督者および/または倉庫管理者は、国際運輸の輸送機関と輸送器材に使用される封印番号を定期的に確認しなければなりません。		必須

ID	基準	実施ガイダンス	必須/勧告
6.7	CTPAT の封印検証プロセスでは、高セキュリティ全封印（ボルト/ケーブル）が国際運輸の輸送器材に適切に添付され、設計どおりに動作していることを確認するためにその手順に従う必要があります。この手順は VVTT プロセスと呼ばれます。 V –封印およびコンテナのロック機構を目視し、それらが正常であることを確認。 V –正確さを期するため、出荷書類に照らして封印番号を確認。 T –封印を引っ張り、きちんと取り付けられていることを確認。 T –ボルトシールをねじり回し、構成部品のねじが緩んだり、互いに分離したり、封印の一部が緩んだりしていないことを確認。	ケーブルシールを使う場合、封印が上下に動かなくするために、垂直棒の基部にある長方形のハードウェアを包むように設置する必要があります。 封印が済むと、ケーブルの両側からたるみが全くないことを確認してください。 ケーブルシールの VVTT プロセスでは、ケーブルがぴんと張られていることを確認する必要があります。 きちんと取り付けられたら、ケーブルを引っ張り、ロック機構内にケーブルの滑りがあるかどうかを確認します。	必須

7. 手続き上のセキュリティ –手続き上のセキュリティは、輸出入プロセス、文書化、貨物保管および取扱い要件など多くの局面を包括しています。重要な手続き上のその他の基準は、インシデントの報告と関連法の執行機関への通知に関するものです。さらに、CTPAT では、長期にわたって一定のプロセス維持に役立つからという理由で、手順を書面化することをたいていの場合義務付けています。しかし、これらの書面による手順に必要な詳細情報の量は、企業のビジネスモデルや手順が適用される対象などさまざまな要素により左右されます。

CTPAT は、サプライチェーンで使用される技術が進化し続けていることを認識しています。基準全体で使用される用語は、書面による手順、文書、および用紙を参照していますが、紙ベースが必須ということではありません。これらの基準を満たすために、電子文書、署名、その他のデジタル技術も受け入れ可能です。

このプログラムは、「すべてのサイズに対応する」モデルとして作られていません。各企業は、（独自のリスク評価に基づいて）手順を実施・維持する方法を決定しなければなりません。ただし、セキュリティプロトコル用の別個のマニュアルを作成するよりも、既存の手順にセキュリティプロセスを組み込む方が効果的です。これによって、より持続可能な構造が構築され、サプライチェーンのセキュリティは全員の責任であることを強調するのに役立ちます。

ID	基準	実施ガイダンス	必須 / 勧告
7.1	貨物が一晩、あるいは長期間にわたって輸送準備のため集結される場合、貨物を不正アクセスから保護するための対策を講じなければなりません。		必須
7.2	貨物の集結区域とその周辺区域を定期的に検査して、これらの区域に目に見える害虫が混入していないことを確認しなければなりません。	必要に応じて、餌、わな、他の障壁の使用などの予防手段を使用できます。 雑草の除去や生い茂った植生の減少は、集結区域内の害虫の生息地の除去に役立つ可能性があります。	必須

ID	基準	実施ガイダンス	必須 / 勧告
7.4	コンテナ/ IIT への貨物の積み込み/詰め込みは、警備員/管理者あるいはその他の指定された人員によって監督されるべきです。		勧告
7.5	適切に取り付けられた封印の文書化された証拠として、詰め込みの時点でデジタル写真を撮るべきです。 実行可能な範囲で、これらの画像を検証目的のため宛先に電子的に転送すべきです。	写真の証拠としては、貨物の標示、積み込みプロセス、封印された場所、きちんと行われた封印の証拠を記録するために詰め込みの時点で撮影された写真が含まれます。	勧告
7.6	商品/貨物の通関に使用される全情報が読みやすく、完全・正確であり、情報の交換、損失、あるいは誤った情報の導入から保護され、時間通りに報告されることを保証するための手順が整っていなければなりません。		必須
7.7	紙の文書を使用する場合、不正使用を防止するため、用紙やその他の輸出入関連の文書を保護すべきです。	積荷目録を含む未使用の用紙の保管を確保し、そのような書類の不正使用を防止するために、鍵をかけたファイリングキャビネットを使用するなどの手段を講じることができます。	勧告
7.8	荷送人・その代理店は、船荷証券（BOL）および/または積荷目録が運送業者に提供された情報を正確に反映していることを確認しなければなりません。 BOL と積荷目録は、タイムリーに米国税関国境取締局（CBP）に提出しなければなりません。 CBP に提出された BOL 情報は、運送業者が米国向け貨物を受け取り所持する最初の外国の場所/施設を示さなければなりません。重量と個数は正確でなければなりません。	封印された国際運輸の輸送器材を受け取る際、運送業者は荷送人の配送指示書に記載されている情報に頼る場合があります。 船荷証券（BOL）やその他の輸出書類に電子的に印刷する封印番号を義務付けることは、封印の変更や新しい封印番号に一致させるための関連文書の変更防止に役立ちます。 ただし、特定のサプライチェーンでは、物品は輸送中、外国税関当局、あるいは CBP によって検査される場合があります。 政府が封印を解くと、審査後に IIT に適用される新しい	必須

ID	基準	実施ガイダンス	必須 / 勧告
		封印番号を記録するプロセスが必要になります。 場合によっては、これは手書きで記載できます。	

ID	基準	実施ガイダンス	必須 / 勧告
7.23	CTPAT 参加企業は、施設の内部エスカレーションプロセスの説明を含めて、インシデント報告の書面による手順書を作成しなければなりません。 世界中のあらゆる場所で発生し、参加企業のサプライチェーンのセキュリティに影響を与える不審な活動・セキュリティインシデント（麻薬の押収、密航者の発見など）を報告するために、通知プロトコルを設定しなければなりません。適用される場合には、参加企業は、世界的なインシデントをサプライチェーン・セキュリティ専門家、直近の通関手続地、関連する法執行機関、および影響を受けるサプライチェーンの一部であるビジネスパートナーに報告しなければなりません。 CBP への通知は、輸送機関や IIT が国境を越える前にできるだけ早く行わなければなりません。 通知手順には、通知を必要とする担当者の氏名と電話番号をリストした正確な連絡先情報と、法執行機関の情報を含めなければなりません。連絡先情報が正確であることを確認するために、手順を定期的に再検討する必要があります。	米国税関国境取締局への通知に値するインシデントの例には、以下が含まれます（ただし、これらに限定されません）。 •コンテナ/ IIT あるいは高セキュリティ封印の改ざんの発見。 •輸送機関あるいは IIT の隠された隔室の発見。 •簿外の新しい封印の IIT への適用。 •人や密航者を含む禁制品の密輸。 •輸送機関、機関車、船舶、もしくは航空母艦への無許可の侵入。 •強要、保護のための支払い、脅し、および/または威嚇。 •事業体識別子（すなわち、輸入者記録（IOR）番号、標準運送業者アルファ（SCAC）コードなど）の不正使用。	必須
7.24	無許可/身元不明の人物を特定し、異議を申し立て、対処するための手順を整えなければなりません。 人員は、未知/無許可の人物に抗議するためのプロトコル、状況への対応方法、および施設から無許可の個人を排除する手順を知らなければなりません。		必須

ID	基準	実施ガイダンス	必須 / 勧告
7.25	CTPAT 参加企業は、セキュリティ関連の問題を匿名で報告するメカニズムを設定すべきです。 申し立てを受け取ったら、捜査すべきであり、該当する場合は是正措置を講じるべきです。	懸念が匿名で報告される可能性があることを報告者が知っている場合、盗難、詐欺、内部陰謀などの内部問題がより容易に報告される可能性があります。 参加企業は、自分の行動に対する報復を恐れる場合に匿名を維持できるホットラインプログラムあるいは同様のメカニズムを設定することができます。 報告は、各報告項目が捜査され、是正措置が取られたことを文書化する証拠として保管することを薦めます。	勧告
7.27	不足、過剰供給、その他の重大な不一致や異常はすべて、必要に応じて捜査・解決されなければなりません。		必須
7.28	到着貨物は、貨物の積荷目録に記載された情報と照合すべきです。 出発貨物は、購入注文・配達注文に照らして検証すべきです。		勧告
7.29	特定の貨物に割り当てられた封印番号は、出発前に荷受人に送信すべきです。		勧告
7.30	封印番号は、船荷証券あるいはその他の出荷書類に電子的に印刷すべきです。		勧告
7.37	参加企業は、重大なセキュリティ・インシデント発生後、インシデントに気付いた直後に、サプライチェーンが侵害された可能性がある場所を判定するために、インシデント事後分析を開始しなければなりません。 この捜査は、政府の法執行機関が実施する既知のいかなる捜査も妨害/干渉してはなりません。 企業のインシデント事後分析の結果は文書化し、可能な限り早く完了し、法執行機関当局が許容する場合には、	セキュリティ・インシデントとは、セキュリティ措置が迂回され、回避され、または違反された結果、犯罪行為が発生したか発生するであろうところの侵害のことです。セキュリティ・インシデントには、テロ行為、密輸（麻薬、人間、その他）および密航者の存在を含みます。	必須

ID	基準	実施ガイダンス	必須 / 勧告
	要請に応じて SCSS が利用できるようにしなければなりません。		

8. 農業セキュリティ –農業は、米国最大の産業であり雇用部門です。侵略的で破壊的な害虫や疾病を宿すかもしれない土壌、肥料、種子、植物および動物材料などの外来動植物汚染物質の導入により脅かされている産業でもあります。全輸送機関ならびに全種類の貨物の汚染物質を除去することにより、CBP の貨物保留、遅延、商品の返品・処理が低減できる可能性があります。CTPAT の農業要件への遵守を確保することは、米国の主要産業と世界全体の食料供給を保護することにも役立ちます。

重要定義: 害虫汚染 –国際海事機関は、害虫汚染を、目に見える形の動物、昆虫、または他の無脊椎動物（生死を問わず、卵殻や浮遊粘着物の塊を含むライフサイクルのあらゆる段階）、あるいは動物由来の有機物質（血液、骨、毛、肉、分泌物、排泄物を含む）、生育可能か否かを問わず植物・植物製品（果物、種子、葉、小枝、根、樹皮を含む）、あるいは真菌を含むその他の有機材料、もしくは土壌や水であって、そのような製品は、国際輸送手段（すなわち、コンテナ、ユニット積載装置など）内の明示された貨物ではないものと定義しています。

ID	基準	実施ガイダンス	必須 / 勧告
8.1	CTPAT 参加企業は、ビジネスモデルに従って、木材包装材（WPM）規制への遵守を含め、目に見える害虫汚染を防ぐ目的での	WPM は、商品の支持、保護、あるいは運搬に使用される木材・木材製品（紙製品を除く）として定義されます。 WPM には、パレット、クレート、ボックス、リール、ダンネージなどの品目が含まれます。これらの品目は、害虫の駆除に十分な処理・対応を受けていない可能性がある原木でたいてい作られているため、害虫の侵入と拡散の経路になっています。特にダンネージは、害虫の侵入と拡散のリスクが高いことが示されています。	必須

ID	基準	実施ガイダンス	必須 / 勧告
	手順を文書化しなければなりません。 目に見える害虫防止対策は、サプライチェーン全体で遵守する必要があります。 WPM に関する措置は、国際植物保護条約（IPPC）の植物検疫措置に関する国際基準 No. 15（ISPM 15）を満たすことが必須です。	IPPC は、国連食糧農業機関が監督する多国間条約であり、害虫や汚染物質の侵入と拡散を防止・制御するために、調整された効果的な措置の確保を目的としています。 ISPM 15 には、WPM に関連する可能性のあるほとんどの害虫の侵入・拡散のリスクを大幅に減らすために、WPM に適用可能な国際的に受け入れられている手段が含まれています。 ISPM 15 は、すべての木材梱包材に影響を及ぼし、皮を剥がした後、臭化メチルで熱処理あるいは燻蒸し、IPPC 遵守の標示を刻印・ブランド化することを義務付けています。この遵守の標示は、通称「小麦のスタンプ」と呼ばれています。 ISPM 15 の対象外の製品は、紙、金属、プラスチック、あるいは木製パネル製品（配向性ストランドボード、硬質繊維版、および合板）などの代替材料から作られているものです。	

第三の焦点分野: 人々と物理的セキュリティ

9. 物理的セキュリティ – 貨物取扱施設と保管施設、国際輸送器材の保管区域、および国内外の場所で輸出入書類が準備される施設では、不正アクセスを防ぐ物理的障壁と抑止措置が備えられていなければなりません。

CTPAT の根本理念の一つは柔軟性であり、セキュリティプログラムは各企業の状況に合わせてカスタム化すべきです。物理的セキュリティの必要性は、サプライチェーンにおける参加企業の役割、そのビジネスモデル、およびリスクのレベルによって大きく変化します。
物理的セキュリティ基準は、貨物、極秘機器、および/または極秘情報への不当なアクセスを防止するために役立つ多くの抑止措置/障害を提供します。参加企業はサプライチェーン全体でこうしたセキュリティ対策を採用すべきです。

ID	基準	実施ガイダンス	必須 / 勧告
9.1	トレーラーヤードやオフィスを含む全貨物取扱・保管施設には、不正アクセスを防ぐ物理的な障壁や抑止措置がなければなりません。		必須

ID	基準	実施ガイダンス	必須 / 勧告
9.2	貨物取扱と保管施設の周りの区域は、外周フェンスで囲むべきです。 施設が貨物を取り扱う場合は、内部フェンシングを使用して、貨物と貨物取扱区域を確保すべきです。 リスクに基づいて、追加の内部フェンスで、国内、国際、高価値、および/または有害物質などの様々な種類の貨物を分離すべきです。指定された担当者が定期的にフェンスの完全性と損傷を検査すべきです。 フェンスに損傷が見つかった場合は、できるだけ早く修理すべきです。	フェンスの代わりに、隔壁や、突き通せない、または険しい崖や密集した茂みなどのアクセスを妨げる自然の特徴など、他の許容可能な障壁を使用することができます。	勧告
9.4	車両および/または人員が出入りするゲート（およびその他の出口ポイント）は、人を配置するか、監視する必要があります。 人員と車両は、現地の法律・労働法に従って捜査対象となる場合があります。	適切なアクセスと安全のために、ゲートの数を必要最低限に抑えることを薦めます。 出口の他の箇所は、ゲートのない施設への入口となります。	必須
9.5	民間の乗用車は、貨物の取扱や保管区域内、ならびに輸送機関に隣接して駐車することを禁止すべきです。	フェンスで囲まれた区域および/または稼働区域の外側、あるいは貨物の取扱・保管区域から少なくともかなり離れた場所に駐車場を配置します。	勧告
9.6	適切な照明を施設の内外で、必要に応じて次の区域を含めて提供する必要があります：出入口、貨物取扱と保管区域、フェンスライン、駐車場。	適切な防犯灯を自動的に点灯する自動タイマーや光センサーは、照明器具に加えて役立ちます。	必須

ID	基準	実施ガイダンス	必須 / 勧告
9.7	施設を監視し、極秘区域への不正アクセスを防止するために、セキュリティ技術を活用すべきです。	極秘区域とアクセスポイントを保護/監視するために使用される電子セキュリティ技術には、次のものがあります。 盗難警報システム（外周と内部）—侵入検出システム（IDS）とも呼ばれる、アクセス制御装置、閉回路テレビカメラ（CCTV）を含むビデオ監視システム（VSS）。 CCTV / VSS システムには、アナログカメラ（同軸ベース）、インターネットプロトコルベース（IP）カメラ（ネットワークベース）、記録装置、ビデオ管理ソフトウェアなど。 ビデオ監視の恩恵を受ける保安/極秘区域には、貨物取扱と保管区域、輸入書類が保管される出荷/荷受け区域、IT サーバー、IIT が 検査される国際輸送器材（IIT）のヤードおよび保管区域、封印保管場所が含まれます。	勧告

ID	基準	実施ガイダンス	必須 / 勧告
9.8	物理的セキュリティのためにセキュリティ技術に頼る参加企業は、この技術の使用、保守、および保護を管理する書面の方針と手順を有する必要があります。 これらの方針と手順は最低限、以下を規定しなければなりません。 •技術が制御・管理されている場所へのアクセスは、許可された人員に限定。 •技術を定期的にテスト/検査するために実施される手順。 •検査には、全装置が適切に動作していること、および該当する場合には装置の正しい配置の検証が含まれていること。 •検査と性能テストの結果が文書化されていること。 •是正措置が必要な場合は、できるだけ早く実施し、是正措置を文書化すること。 •これらの検査結果は文書化され、監査目的のために十分な期間保持されること。 第三者の中央監視ステーション（オフサイト）を使用する場合、CTPAT 参加企業は、セキュリティコードの変更、権限のある担当者の追加や削除、パスワードの改訂、システ	セキュリティ技術は、適切に機能していることを確認するために定期的にテストする必要があります。従うべき一般的なガイドラインがあります。 •サービス作業後、ならびに建物・施設の大規模な修理、改変、あるいは追加の行われている期間中とその後にセキュリティシステムをテストする。システムのコンポーネントが意図的もしくは意図なく侵害された可能性がある。 •電話やインターネットサービスに大きな変更を加えた後、セキュリティシステムをテストする。システムの監視センターとの通信能力に影響を与える可能性のあるものは全部再確認する必要がある。 •モーション起動録画などのビデオ設定、動体検知アラート。1 秒あたりの画像数（IPS）と品質レベルが適切に設定されていることを確認。 •カメラのレンズ（またはカメラを保護するドーム）が清潔で、レンズの焦点が合っていることを確認。視界は障害物や明るい光によって制限されてはならない。 •防犯カメラが正しく配置され、適切な位置にあることを確認するためのテストを行う（カメラは意図的あるいは誤って移動された可能性がある）。	必須

ID	基準	実施ガイダンス	必須 / 勧告
	ムへのアクセスや拒否など（それに限定されない）の重要システム機能、認証プロトコルを規定する手順書を持たなければなりません。 セキュリティ技術の方針と手順は、リスクや状況に応じて、毎年、あるいはそれより頻繁に再検討・更新しなければなりません。		
9.9	CTPAT 参加企業は、セキュリティ技術の設計・設置を検討する際に、ライセンス/認定リソースを使用すべきです。	今日のセキュリティ技術は複雑で、急速に進化しています。多くの場合、企業は、誤ったセキュリティ技術を購入して必要な時に効果がないと判ったり、必要以上の費用を支払ったりしています。資格のあるガイダンスを求めることは、購買者が自己のニーズと予算に合った適切な技術オプションを選択するのに役立ちます。 米国電気工事請負業者協会（NECA）によると、米国の 33 州には現在、セキュリティ・警報システムの設置に従事する専門家のライセンス要件があります。	勧告
9.10	全セキュリティ技術インフラは、不正アクセスから物理的に保護しなければなりません。	セキュリティ技術インフラには、コンピュータ、セキュリティソフトウェア、電子制御パネル、ビデオ監視・閉回路テレビカメラ、カメラの電源およびハードドライブ構成部品、録画が含まれます。	必須
9.11	セキュリティ技術システムは、直接電力が予測なく失われた場合にもシステムが動作し続けることを可能にする代替電源で構成すべきです。	セキュリティを侵害しようとする犯罪者は、セキュリティ技術を迂回するために、セキュリティ技術への電力を無効にしようとする場合があります。 したがって、セキュリティ技術の代替電源を用意することが重要です。 代替電源は、補助発電源	勧告

ID	基準	実施ガイダンス	必須 / 勧告
		やバックアップ電池です。 バックアップ発電機は、照明などの他の重要なシステムにも使用できます。	
9.12	カメラシステムが配置されている場合、カメラは施設の敷地と外部の影響を受けやすい区域を監視し不正アクセスを阻止すべきです。 外部の影響を受けやすい区域への不正アクセスについて会社に警告するには、警報を使用すべきです。	外部の影響を受けやすい区域には、必要に応じて、貨物の取扱・保管区域、輸入書類が保管される出荷/荷受け区域、IT サーバー、国際輸送器材（IIT）のヤードと保管エリア、IIT が検査される区域、および封印保管区域が含まれる場合があります。	勧告
9.13	カメラシステムが配置されている場合、カメラは、輸出入プロセスに関連する施設の主要な領域をカバーするように配置しなければなりません。 カメラは、利用可能な最高の画質設定で録画し、24 時間 7 日間常時録画するように設定すべきです。	カメラが施設の制御内で物理的な「管理の連鎖」をできるだけ記録できるようにするには、カメラを正しく配置することが重要です。 リスクに基づいて、重要区域・プロセスには、貨物の取扱いと保管、発送/受け取り、 貨物の積み込みプロセス、封印プロセス、 輸送機関の到着/出口、IT サーバー、コンテナ検査（セキュリティと農業）、封印保管、および国際出荷の確保に関係するその他の分野が含まれる場合があります。	必須
9.14	カメラシステムが配置されている場合、カメラには「操作/記録の故障」状態を通知する警報/通知機能が必要です。	ビデオ監視システムの故障は、犯罪のビデオ証拠を残すことなくサプライチェーンを侵害するために何者かがシステムを無効にした結果である可能性があります。 操作ができなくなると、事前に指定された人に電子通知が送信され、装置にすぐに注意が必要であることを通知されます。	勧告

ID	基準	実施ガイダンス	必須 / 勧告
9.15	カメラシステムが配置されている場合、カメラ映像の定期的かつ無作為な再検討を（管理層、セキュリティ、またはその他の指定された担当者によって）実施し、貨物のセキュリティ手順が法律通りに適切に守られていることを確認しなければなりません。 再検討の結果は書面で要約し、実施した是正措置を含めなければなりません。 結果は、監査目的に十分な期間保持しておく必要があります　。	カメラ映像が特定の目的のため（セキュリティ侵害などの後の捜査の一環として）のみ再検討される場合には、カメラを持つことの完全な恩恵が享受されていません。カメラは捜査ツールであるだけではありません。積極的に活用すると、セキュリティ侵害が発生すること自体を当初から防ぐことに役立ちます。 貨物が安全に保管され、全セキュリティプロトコルが守られていることを確認するために、保管の物理的連鎖に関する映像の無作為な再検討を実施してください。再検討しうるプロセスの例は次のとおりです。 •貨物取り扱い活動 •コンテナ検査 •積み込みプロセス •封印プロセス •輸送機関の到着/出口 •貨物の出発など 再検討の目的：再検討は、確立されたセキュリティプロセスの全体的な遵守と有効性を評価し、ギャップや認められた弱点を特定し、セキュリティプロセスの改善を支援する是正措置の規定することを目的としています。リスクに基づいて（以前のインシデントや、積荷港でのセキュリティプロトコルに従わなかった従業員に関する匿名の報告など）、参加企業は定期的に再検討を行うことができます。 書面による要約に含める項目： •再検討の日付	必須

ID	基準	実施ガイダンス	必須 / 勧告
		•再検討された映像の日付 •録画を行ったカメラ/区域 •発見事項の簡単な説明 •必要ならば、是正措置	
9.16	カメラを使用中の場合、重要な輸出入プロセスを対象とする映像の記録は、監視対象の貨物に関して、捜査が完了するのに十分な時間保有しておくべきです。	違反が発生した場合、捜査の実施が必要となりますが、梱包（輸出用）および積荷/封印プロセスを対象とするカメラ映像を保持することは、サプライチェーンが侵害された可能性がある場所を発見する上で最も重要です。 監視のために、CTPAT プログラムでは、出荷が最初の配送地に到着してから最低 14 日間を割り当てることを推奨しています。 これは、税関を通過した後にコンテナが最初に開かれる場所です。	勧告

10. 物理的アクセスの管理 –アクセス管理は施設/区域への不正アクセスを防止し、従業員・訪問者の管理を維持し、企業資産を保護するために役立ちます。アクセス管理は全入口で全従業員、訪問者、サービス提供業者、納入業者の身元確認を含めています。

ID	基準	実施ガイダンス	必須/ 勧告
10.1	CTPAT 参加企業は、ID バッジとアクセス装置の提供、変更、および削除方法を管理する文書化された手順を有する必要があります。	アクセス装置には、従業員身分証明バッジ、訪問者と納入業者の一時交付バッジ、生体認証システム、近接キーカード、コード、およびキーが含まれます。 従業員が会社を辞める場合、出口チェックリストを使用すると、全アクセス装置が返却および/または無効化の確認に役立ちます。 従業員がお互い	必須

ID	基準	実施ガイダンス	必須/勧告
	該当する場合は、確実な身分証明とアクセス制御を目的として、個人身分証明システムを設置する必要があります。 職務内容あるいは割り当てられた職務に基づいて、極秘区域へのアクセスを制限する必要があります。 アクセスデバイスの取り外しは、従業員が会社を離れたときに行う必要があります。	を知っている中小企業の場合、身分証明システムは必要ありません。 一般に、従業員が 50 人を超える会社では、身分証明システムが必要です。	

ID	基準	実施ガイダンス	必須/勧告
10.2	訪問者、納入業者、サービス提供業者は、到着時に写真付き身分証明書を提示し、訪問の詳細を記録するログを保持しなければなりません。 全訪問者に付き添いを付けるべきです。 さらに、全訪問者とサービス提供業者に一時的な身分証明書を発行すべきです。 一時的な身分証明書を使用する場合は、訪問中は常に目で見えるように身に着けていなければなりません。 登録ログには以下が含まれていなければなりません。 •訪問日 •訪問者の氏名 •写真付き身分証明書の確認（免許証や国民 ID カードなどの確認済みのタイプ）。 通常の納入業者などの頻繁によく知られている訪問者は、写真付きの身分証明書を差し控えることが可能だが、それでも施設にログインとログアウトしなければならない。 • 到着時刻 •会社の連絡先 • 出発時間		必須

ID	基準	実施ガイダンス	必須/勧告
10.3	貨物を受け取ったり、引き渡したりする前に、貨物を配達・受領する運転手の身元を明確に確認しなければなりません。運転手は、身分を証明するためにアクセスを許可する施設の従業員に政府発行の写真付き身分証明書を提示しなければなりません。 政府発行の写真付き身分証明書の提示が不可能な場合、施設の従業員は、荷物を受け取る運転手を雇用している高速道路運送会社が発行した承認済みの写真付き身分証明書を受け入れることができます。		必須
10.4	貨物を積み込む際に、運転手を登録し、輸送の詳細を記録するために、貨物集荷ログに記入しなければなりません。 貨物を引き取るために運転手が施設に到着すると、施設の従業員はそれを貨物集荷ログに登録しなければなりません。 出発時には、運転手をログアウトしなければなりません。 貨物ログは安全に保持する必要があり、運転手がログにアクセスできないようにしなければなりません。 貨物引き渡しログには、次の項目が記録されるべきです。 •運転手の氏名 •到着日時 • 雇用主 •トラック番号 •トレーラー番号 • 出発時間 •出発時に貨物に添付されている封印番号	訪問者ログは、追加情報が記録されている限り、貨物ログを兼ねることができます。	必須

ID	基準	実施ガイダンス	必須/勧告
10.7	到着前に、運送業者は、予定された集荷のための到着予定時刻、運転手の氏名、トラック番号を施設に通知すべきです。運営上これが実行可能な場合、CTPAT 参加企業は、予約のみで配達と集荷を許可すべきです。	この基準は、荷送人と運送業者が架空の集荷を回避するために役立ちます。 架空の集荷とは、偽造 ID を使用するトラック運転手や貨物窃盗を目的に設定された架空の事業者を含む詐欺による貨物の盗難をもたらす犯罪計画です。 運送業者が特定の施設から商品を引き取る定期的な運転手を抱えている場合、施設では運転手のリストを写真とともに管理することを薦めます。 したがって、どの運転手が来ているかを会社に知らせることができない場合でも、会社は運転手が施設から貨物を引き取ることが承認済みであることを確認できます。	勧告
10.8	到着する荷物と郵便物は、収容許可前に密輸品を定期的に検査する必要があります。	このような密輸品の例には、爆発物、違法薬物、通貨が含まれますが、これらに限定されません。	勧告
10.10	警備員が活用される場合、警備員の作業指示は、文書化された方針と手順に含まれていなければなりません。 経営陣は、監査と方針の検討を通じて、これらの手順の遵守と適切性を定期的に検証しなければなりません。	警備員はどの施設でも活用できますが、製造現場、港湾、物流センター、国際輸送器材の保管場、コンソリデーター、およびフォワーダーの作業現場でたいてい活用されます。	必須

11. 人的セキュリティ –企業の人的資源は最も重要な資産の一つですが、最も脆弱なセキュリティ・リンクの一つでもありえます。このカテゴリーの基準は、従業員の審査や雇用前の身元確認などの問題に焦点を当てています。セキュリティ侵害の多くは、内部の陰謀により引き起こされます。これは１人あるいは複数の従業員が共謀して、サプライチャーンへの侵入の許可を得ることを目的としてセキュリティ手順を迂回する行為です。そのため、参加企業は、デューデリジェンスを実施して、極秘職務に従事する従業員が頼りになり、かつ信頼できることを確認する必要があります。 極秘役職には、貨物やその書類を直接扱うスタッフ、および

極秘区域や機器へのアクセスの管理に関与するスタッフが含まれます。 そうした役職には、発送、受け取り、郵便室の職員、運転手、派遣、警備員、荷物の割り当て、輸送の追跡、および/または封印管理が含まれますが、これらに限定されません。

ID	基準	実施ガイダンス	必須/勧告
11.1	従業員候補者を検査し、現在の従業員を定期的に点検するために、文書化されたプロセスを整えなければなりません。雇用履歴や照会先などの申請情報は、法律の下で許可され可能である範囲で、雇用前に検証する必要があります。	CTPAT は、特定の国の労働法やプライバシー法により、申請情報の全てを検証できない場合があることを認識しています。 ただし、認められる場合には、申請情報を検証するためにデューデリジェンスが期待されます。	必須

ID	基準	実施ガイダンス	必須/勧告
11.2	適用される法的制限、および犯罪歴データベースの利用可能性に従って、従業員の経歴審査を実施すべきです。 職位の極秘度に基づいて、従業員の審査要件は、一時雇用労働者と請負業者にまで拡大すべきです。 雇用後は、特定の理由や従業員の立場の極秘度に基づいて定期的な再調査を実施すべきです。 従業員の身元調査には、従業員の身元と犯罪歴の検証を含めるべきです。これには、都市、州、省、および国のデータベースを含めるべきです。 CTPAT 参加企業とそのビジネスパートナーは、現地の法律で許可されているように、採用決定において身元調査結果を考慮すべきです。 身元調査は、身元と犯罪歴の確認に限定されません。 よりリスクの高い分野では、より一層詳細な調査が必要になる場合もあります。		勧告
11.5	CTPAT 参加企業は、期待されていることを含めて、かつ許容可能な行動を定義する従業員の行動規範を有する必要があります。 罰則と懲戒手続きは行動規範に含まれなければなりません。 従業員/請負業者は、行動規範に署名することにより、読んで理解したことを確認しなければならず、この確認は書類の裏付けとして、従業員ファイルに保管しなければなりません。	行動規範は、企業を保護し、従業員に何が期待されているかを伝えます。 その目的は、企業が受け入れられる行動基準を作成・保持することです。 企業がプロフェッショナルなイメージを開発し、強力な倫理文化を確立するのに役立ちます。 小さな会社でも行動規範が必要です。 ただし、立案が複雑である必要はなく、複雑な情報を入れる必要もありません。	必須

12. 教育、訓練および警戒意識 –CTPAT のセキュリティ基準は、階層化されたセキュリティシステムの基盤を形成することを　目的としています。セキュリティの一つの層が破られた場合、別の層がセキュリティ違反を防ぐか、企業に違反を警告すべきです。階層化されたセキュリティシステムの実施と維持には、複数の部門と様々な担当者の積極的な参加と支援が必要です。セキュリティプログラムを維持するための重要な側面の一つは、人員訓練です。脅威とは何か、会社のサプライチェーンを保護する上でその役割がどのように重要であるかを従業員に教育することは、サプライチェーン・セキュリティプログラムの成功と耐久性にとって重要な側面です。 さらに、従業員がセキュリティ手順の実施理由を理解すると、従業員がそれを遵守する可能性がはるかに高くなります。

ID	基準	実施ガイダンス	必須 / 勧告
12.1	参加企業は、テロリストや禁制品密輸業者によって悪用される可能性のあるサプライチェーンの各箇所で、施設、輸送機関、貨物セキュリティの脆弱性を認識し、警戒意識を育成するためのセキュリティ訓練と意識向上プログラムを確立し、維持しなければなりません。訓練プログラムは包括的であり、CTPAT の全セキュリティ要件を網羅しなければなりません。極秘な職位にある人員は、その職位を担う責任に合わせた追加の専門訓練を受けなければなりません。 セキュリティプログラムの重要な側面の一つは訓練です。セキュリティ対策が実施されている理由を理解している従業員は、遵守する可能性が高くなります。セキュリティ訓練は、必要に応じて、定期的に職務と職位に基づいて従業員に提供しなければならず、新入社員はオリエンテーション/職務技能訓練の一環としてこの訓練を受けなければなりません。	トレーニングのトピックには、アクセス制御の保護、内部陰謀の認識、および疑わしい活動とセキュリティインシデントの報告手順が含まれます。 可能な場合、専門トレーニングには実践的な実演を含める必要があります。 実践的な実演を行う場合、講師は、受講者がプロセスを実演する時間を確保する必要があります。 CTPAT の目的のために、極秘な役職としては、輸入/輸出貨物あるいはその文書を直接扱うスタッフ、および極秘区域や機器へのアクセスの制御に関与するスタッフが含まれます。そのような役職には、発送、受け取り、郵便室の職員、運転手、派遣、警備員、荷物の割り当て、輸送の追跡、および/または封印管理が含まれますが、これらに限定されません。	必須

ID	基準	実施ガイダンス	必須 / 勧告
	参加企業は、訓練ログ、出勤シート（勤務名簿）、あるいは電子訓練記録などの訓練の証拠を保持しなければなりません。訓練記録には、訓練の日付、参加者の氏名、および訓練のトピックを含めるべきです。		

ID	基準	実施ガイダンス	必須 / 勧告
12.2	国際運輸の輸送機関と輸送器材（IIT）を空の状態でセキュリティ・農業検査を実施する運転手やその他の要員は、セキュリティ・農業の両方の目的で輸送機関/ IIT を検査するための訓練を受けなければなりません。 インシデントやセキュリティ違反の後、もしくは企業の手順に変更があった場合、必要に応じて、再教育訓練を定期的に実施しなければなりません。 検査訓練には、次のトピックを含めなければなりません。 •隠された区画空間の兆候 •自然の窪みに隠された密輸品 •害虫汚染の兆候		必須
12.4	CTPAT 参加企業は、行われた訓練が訓練目標を全て満たしていることを確認するための措置を講じるべきです。	訓練を理解し、その訓練を自分の職位で活用できるようにすること（極秘職の従業員向け）は非常に重要です。 テストやクイズ、シミュレーションの演習/教練、もしくは手順の定期監査などは、訓練の有効性を判断するために参加企業が実施できる措置の一部です。	勧告
12.8	必要に応じて、その職務および/または職位に基づいて、従業員は会社のサイバーセキュリティの方針と手順に関する訓練を受けなければなりません。 これには、従業員がパスワード/パスフレーズとコンピュータアクセスを保護する必要性を含めなければなりません。	質の高い訓練は、サイバー攻撃に対する脆弱性を低減するために重要です。 強力なサイバーセキュリティ訓練プログラムは、通常、単に電子メールやメモを介してではなく、正式な環境設定で該当する担当者に提供されるものです。	必須

ID	基準	実施ガイダンス	必須 / 勧告
12.9	セキュリティ技術システムを運用・管理する担当者は、特定の分野で運用・維持の訓練を受けなければなりません。 同様のシステムでの過去の経験は容認できます。 操作マニュアルおよびその他の方法による自己訓練は容認できます。		必須
12.10	セキュリティインシデントと不審活動を報告する方法について職員を訓練しなければなりません。	セキュリティインシデントや不審活動を報告する手順は、セキュリティプログラムの非常に重要な側面です。 インシデントの報告方法に関する訓練は、全体的セキュリティ訓練に含めることができます。 専門的な訓練モジュール（職務に基づく）には、報告の手順に関するより詳細な訓練を含めることができます。この中には、報告内容、報告対象者、インシデントの報告方法、報告完了後の対応などプロセスの詳細が含まれます。	必須

出版物番号: 1078-0420