中間取りまとめ②に位置付ける情報セキュリティ対策等の推進のための制度的措置（案）

国土交通省

資料２－２

緊急的対策

事案発生直後の対策（Ｒ５．７．７～　実施中）

○港湾運送事業者、港湾運営会社、ふ頭会社、港湾管理者を通じて関係事業者に対し、「物流分野における情報セキュリティ確保に係る安全ガイドライン」を参考に必要な対策を講じるよう注意喚起を実施。

中間取りまとめ①を踏まえた緊急的対策（Ｒ５．９．２９～ 実施中）

○専門家の意見を踏まえ、具体的な情報セキュリティ対策、システム障害発生時の対応策を中間取りまとめ①で示す。

○中間とりまとめ①後、港湾運送事業者に通知し、説明会等により周知の上、取組状況をフォローアップ

➡ **専門家の知見を踏まえた港湾分野における最新のサイバーセキュリティ対策を事業者に周知徹底**

制度的措置

TOS：ターミナルオペレーションシステム

港湾運送事業法の観点

○コンテナターミナルにおいて一般港湾運送事業者が使用するTOSについて、①TOSの情報セキュリティ対策の状況を的確に把握し、②TOSの情報セキュリティ対策の強化・底上げを図ることが必要。

○港湾運送事業への参入等に際して審査を受ける必要がある事業計画にTOSの概要や情報セキュリティの確保に関する事項の記載を求める。

➡ **TOSの情報セキュリティ対策の確保状況を国が審査する仕組みの導入**

サイバーセキュリティ基本法の観点

○「重要インフラのサイバーセキュリティに係る行動計画」を改定し、重要インフラ分野に「港湾分野」を位置づける方向で検討する。

○コンテナターミナルにおけるTOSを含む港湾分野に焦点を当てた情報セキュリティガイドラインを作成する。

➡ **官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進**

経済安全保障の観点

○TOSについては、その機能が停止・低下し、港湾運送事業者の行う荷役作業に支障が生じた場合、影響が甚大となるおそれがあり、経済安全保障の観点からも国として積極的な関与を行うことを検討することが必要。

○その際、経済安全保障推進法の対象事業とするかどうかは、法の趣旨も十分に踏まえつつ引き続き検討。

港湾運送事業法によるTOSのセキュリティ対策

国土交通省

（名古屋港の事案より）
コンテナターミナルのTOSが停止した場合、TOSを介さずに荷役を継続することが困難なターミナルが生じると考えられる

港湾運送の安定的な提供を図る観点から、**①TOSの情報セキュリティ対策の状況を的確に把握し、②TOSの情報セキュリティ対策の強化・底上げを図ることが必要**

【TOSの情報セキュリティの確保状況を国が審査する仕組みの導入】

港湾運送事業への参入等に際して審査を受ける必要がある**事業計画にTOSの概要や情報セキュリティの確保に関する事項の記載を求める**

⇒事業計画に定める業務を確保することを通じ、情報セキュリティ対策を確保

【制度設計に際しての留意点】
- 事業計画に記載するTOSの概要や情報セキュリティの確保に関する事項として何を求めるのか。
- TOSの使用者と所有者が異なる場合に情報セキュリティ対策の確保の実効性をどのように担保するのか。
- コンテナターミナルの重要性やシステムの依存度が異なる中で、情報セキュリティ対策の設定条件及び情報セキュリティ対策のレベルをどうするのか。
- 国の関与については、港湾運送事業者に過度な負担とならないよう、港湾運送事業の継続のために真に必要なものに限定する。

サイバーセキュリティ基本法における重要インフラの位置付けと行動計画

国土交通省

サイバーセキュリティ基本法における重要インフラの位置付け

重要インフラの定義

重要社会基盤事業者

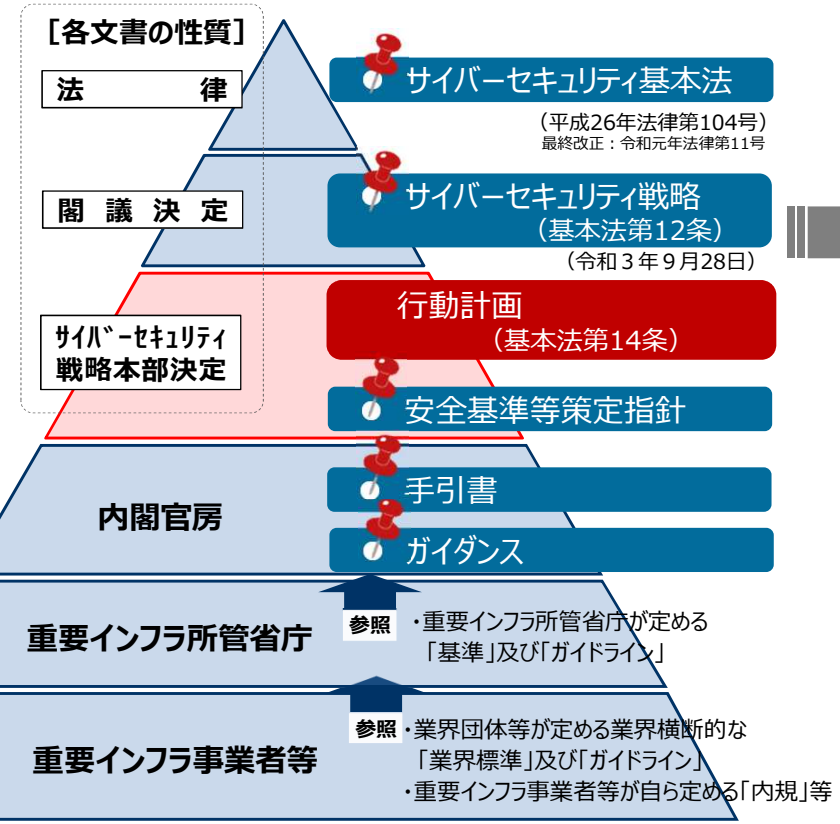
国民生活及び経済活動の基盤であって、その**機能が停止し、又は低下**した場合に国民生活又は経済活動に**多大な影響を及ぼす**おそれが生ずるものに関する事業を行う者

重要インフラの責務

（重要社会基盤事業者の責務）

第６条　重要社会基盤事業者は、基本理念にのっとり、その**サービスを安定的かつ適切に提供**するため、サイバーセキュリティの重要性に関する関心と理解を深め、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力する**よう努めるものとする。

重要インフラ防護に関する戦略・指針等



「重要インフラのサイバーセキュリティに係る行動計画」

✓ **重要インフラ防護に係る基本的な枠組み**を定めた政府と重要インフラ事業者との**官民共通の行動計画**。**国、重要インフラ事業者等が取り組むべき事項が規定**。

主な取り組み

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用

自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

「重要インフラのサイバーセキュリティに係る行動計画」における関係主体において取り組むべき事項

国土交通省

第2回検討会における意見

・脆弱性対策を「定期的」に取るだけで良いのか。随時確認する必要がある。

・インターネットを介さない、専用線やNAT経由のものについてもファイアーウォールを入れるべき。

・国際的視点も重要。国際的なガイドラインをレビューして、活用するのも手である。

最新情報やトレンドを反映した対策の実施

・バックアップはサイバー攻撃によっても破壊されないように場所、頻度等にすべき。

適切なバックアップ等による事業継続

・多様な関係者がおり、所有者と運用者が異なる共有システムの運用は難しいのではないか。

・共有システムの運用は個々の企業のシステムと比較して、対策不足の可能性がある。

多様な関係者などの港湾の特性を踏まえた体制の構築

重要インフラ所管省庁において取り組むべき事項（一部抜粋）

✓ **安全基準等の整備及び浸透**

- 定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて安全基準等の改定を実施。
- 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透に向けた取組を実施。

✓ **情報共有体制の強化**

- 内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。

重要インフラ事業者等において取り組むべき事項（一部抜粋）

✓ **障害対応体制の強化**

- 経営層、CISO、戦略マネジメント層、システム担当者の役割と責任に基づく、組織一丸となった対応。
- インシデントの発生時に対処できる体制の整備。
- 日々の運用で、発見した脅威や脆弱性を払拭するような管理策の実施。
- BCP及びIT-BCP 、CSIRT等、インシデントの発生時に対処できる体制の整備

✓ **安全基準等の整備及び浸透**

- 安全基準等を踏まえ、サイバーセキュリティの確保の取組やそのための環境整備を検討。

✓ **情報共有体制の強化**

- 関係者、関係省庁と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。
- 攻撃手法及び復旧手法に関する情報等の収集。
- 内閣官房が提供する情報疎通機能の確認等を活用するなどして、自らの情報共有体制を強化。

✓ **リスクマネジメントの活用**

- 自組織に適した防護対策について、計画、実施、評価、改善(PDCA)のサイクルを繰り返し、継続的な改善の実施。

✓ **防護基盤の強化**

- 分野横断的演習への参加。
- 分野横断的演習を通じて、自組織の体制や内規、リスクマネジメント等が有効に機能しているかの見直しを実施。

重要インフラ分野への【港湾】の位置づけ

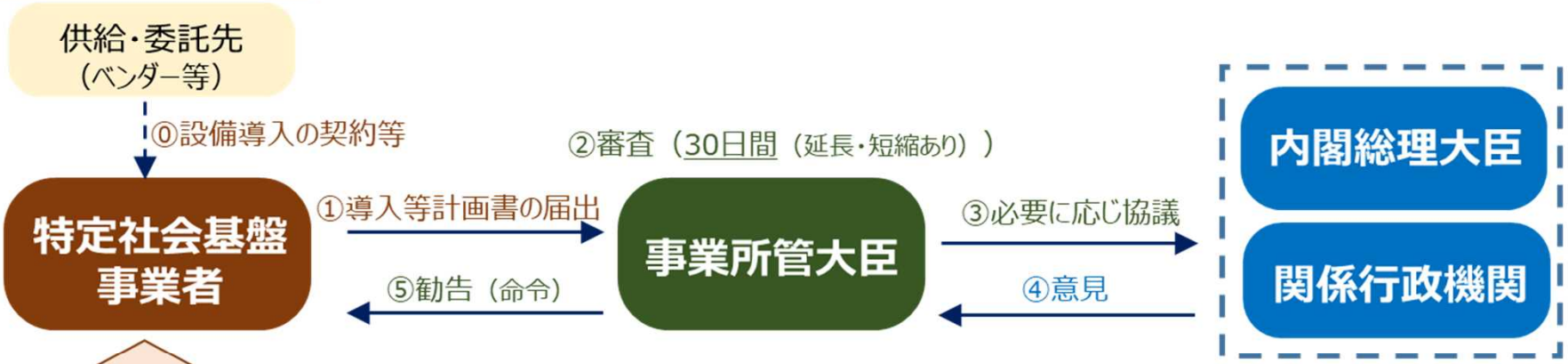
経済安全保障推進法（基幹インフラの安定的な提供の確保関係）の概要

国土交通省

基幹インフラの安定的な提供の確保に関する制度の概要

- 基幹インフラの重要設備が役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、国が一定の基準のもと、**基幹インフラ事業（特定社会基盤事業）・事業者（特定社会基盤事業者）を指定**し、国が指定した**重要設備（特定重要設備）の導入・維持管理等の委託をしようとする際には、事前に国に届出を行い、審査を受ける制度**を構築。本年11月に法を施行し、**来年５月制度運用開始**。
- 国は、届け出られた計画書に係る特定重要設備が妨害行為の手段として使用されるおそれが大きいと認めるときは、当該計画書を届け出た者に対し、妨害行為を防止するため必要な措置を講じた上で重要設備の導入等を行うこと等を勧告（命令）できる。

制度のスキーム



(1) **対象事業**…法律で次の14分野を外縁として規定。それぞれの分野について、必要な範囲に細分化し**政令**で絞り込み。

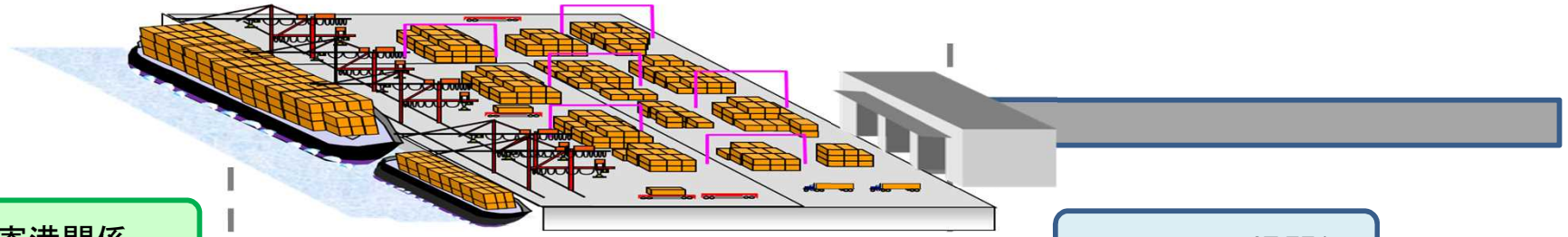
1.電気	2.ガス	3.石油	4.水道	5.鉄道
6.貨物自動車運送	7.外航貨物	8.航空	9.空港	10.電気通信
11.放送	12.郵便	13.金融	14.クレジットカード	

(2) **対象事業者（特定社会基盤事業者）**…絞り込んだ事業ごとに、事業所管大臣が、**省令**で基準を作成し、該当する者を指定・**告示**。

（出典）内閣府作成資料

【参考】コンテナターミナルの機能提供に必要なシステムについて

国土交通省



船舶寄港関係

トラック入退場関係

入出港手続
船社・代理店
↓
港湾管理者
対象：船舶単位

係留施設等利用許可手続
船社・代理店・港運
↓
港湾管理者（指定管理者）
港湾運営会社
対象：主に船舶単位

主に船舶単位の処理のため、件数が少ない。

国際船舶・港湾保安法に基づくゲートにおける出入管理
トラックドライバー
↓
埠頭保安管理者
対象：トラックドライバー単位

国が「出入管理情報システム」を保有しており、情報セキュリティ対策を自ら実施している。

港湾運送事業者の荷役に係るターミナルオペレーション関係

港湾運送事業者の荷役業務
〔 港湾運送事業者 〕
対象：コンテナ単位

・コンテナ単位でデータ管理をする必要があり、処理すべき情報が膨大。
・ターミナルオペレーションシステム（TOS）が有する機能により、これらの情報を処理。
→コンテナターミナルの機能の安定的な提供に不可欠

（ターミナルオペレーションシステム（TOS）の機能）

本船プランニング	ヤードプランニング	ヤードオペレーション
船舶への貨物の積込、船舶からの貨物の取卸に対する計画の管理	コンテナターミナル内におけるコンテナの配置計画等の管理	コンテナターミナル内におけるコンテナの管理・監視等

全体管理　各機能を総合的に管理するとともに、ゲート管理や外部システムとの連携を行う

【参考】港湾荷役に用いられている標準的なシステムについて

国土交通省

埠頭の類型		荷役に用いられているシステム
コンテナ埠頭		○ターミナルオペレーションシステム（TOS） 比較的取扱貨物量の多いターミナルに導入※1
フェリー・RORO 埠頭		＜複合一貫輸送＞【※2】 ○ターミナルオペレーションシステム（TOS） ○車両管理システム　○貨物予約システム 一部のターミナルで使用※1
		＜完成自動車輸送＞ ○ターミナルオペレーションシステム（TOS） 企業の専用ターミナルの一部に当該企業が導入※1
バルク埠頭		○ターミナルオペレーションシステム（TOS） 企業の専用ターミナルの一部に当該企業が導入※1

※1　システムを用いて荷役を行っている事業者においても、紙、表計算ソフト等を用いて荷役可能としている者あり。

※2　フェリー・ROROでの輸送割合
【内航】：1.1%　（2021年　全国貨物純流動調査（3日間調査）より国土交通省港湾局作成）
国内の貨物純流動のうち主にフェリー・RORОによって輸送されたものの割合
【外航】：0.9%　（2018年　全国輸出入コンテナ貨物流動調査より国土交通省港湾局作成）
外貿コンテナ取扱貨物量のうちフェリー・RORОによって輸送されたものの割合