コンテナターミナルにおける情報セキュリティ対策等委員会　取りまとめ
名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策および情報セキュリティ対策等の推進のための制度的措置について（概要）

国土交通省

コンテナターミナルにおける情報セキュリティ対策として特に留意すべき点を整理し、緊急に実施すべき対応策及び情報セキュリティ対策等の推進のための制度的措置について、本委員会としての考え方を取りまとめたもの。

名古屋港事案の検証

（1）名古屋港事案の検証、（2）感染経路、（3）問題点の抽出と改善点、（4）グッドプラクティス

ターミナルオペレーションシステムに必要な情報セキュリティ対策

（1）資産の把握
（2）外部との接続
（3）サーバー機器、システム内のネットワーク機器
（4）バックアップ
（5）クラウド利用時の対策
（6）TOSと連携している外部機器への影響
（7）外部委託を行う場合の情報セキュリティの確保

コンテナターミナルの運用に必要な情報セキュリティ体制

（1）組織・体制の確立
（2）情報連絡体制
（3）BCP
（4）情報セキュリティに関する情報収集
（5）情報セキュリティの意識の向上及び情報セキュリティ教育・訓練
（6）TOS利用契約時における責任分界、保険加入の検討
（7）脆弱性や設定不備の定期検査
（8）情報セキュリティ対策の監査

情報セキュリティ対策等の推進のための制度的措置

○港湾運送事業法に基づく措置　→TOSの情報セキュリティ対策を国が審査する仕組みの導入
○港湾の情報セキュリティ対策を効果的に実施するための措置　→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からの措置　→経済安全保障の観点からも国として積極的に関与

◆ 名古屋港事案の検証

【感染経路】
保守用VPNを通じて物理サーバにランサムウェアが侵入し、サーバ情報が暗号化されたものと考えられる一方で、VPN経由以外での侵害の可能性についても精査すべき

【主な問題点】
〇保守作業に利用する外部接続部分のセキュリティ対策が見落とされていたこと
〇サーバ機器及びネットワーク機器の脆弱性対策が不十分であったこと
〇バックアップの取得対象と保存期間が不十分であったこと
〇システム障害発生時の対応手順が未整備であったこと　等

【主な評価点】
〇事案発生から丸2日半という短期間で復旧が図られたこと
〇システムを使用せずにマニュアル作業で船舶との間の荷役が継続されたこと　等

◆ ターミナルオペレーションシステムに必要な情報セキュリティ対策

〇システムの機器構成、ネットワーク構成、外部との接続状況等の把握
〇サーバやネットワーク機器の外部接続に関する設定の見直し
〇セキュリティ対策ソフトの導入、ソフトウェアの定期的な更新
〇システムログを含むバックアップの取得と適切な取得頻度・保存期間・保存場所の設定
〇外部委託を行う場合の情報セキュリティの確保　等

◆ コンテナターミナルの運用に必要な情報セキュリティ体制

〇最高情報セキュリティ責任者及び情報セキュリティ担当者の指定
〇セキュリティインシデント対応手順の策定及びセキュリティインシデント対応訓練の実施
〇情報連絡体制の構築、システム障害を想定した事業継続計画の策定
〇情報セキュリティに関する情報の収集
〇関係者の情報セキュリティ意識の向上及び情報セキュリティ教育・訓練等の実施
〇脆弱性や設定不備の検査及び情報セキュリテイ対策の監査の定期的な実施　等

情報セキュリティ対策等の推進のための制度的措置

国土交通省

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。

情報セキュリティ対策等の周知徹底（Ｒ５．９．２９～ 実施中）

○専門家の意見を踏まえた、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（中間取りまとめ①）を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情報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

○コンテナターミナルにおいて一般港湾運送事業者に使用されるTOSの機能が停止・低下し、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る。

○経済安全保障推進法の趣旨も踏まえ、TOSを使用して役務の提供を行う一般港湾運送事業を経済安全保障推進法の対象事業とすることが必要であると考えられる。

➡ **経済安全保障の観点からも国として積極的に関与**