資料３－５

国土交通省におけるサイバーセキュリティに関する取り組み状況

国土交通省　港湾局

令和5年12月

名古屋港コンテナターミナルのシステム障害について

国土交通省

名古屋港統一ターミナルシステム(NUTS)概要

- 名古屋港におけるコンテナの積みおろし作業、搬入・搬出等を一元的に管理するシステム
- 名古屋港の5つのコンテナターミナルにおける荷役機械、各種端末、ゲート等と連携している
- システムの保有者はNUCT※、運用者は名古屋港運協会名古屋港コンテナ委員会ターミナル部会

※NUCT＝名古屋ユナイテッドコンテナターミナル株式会社

経過

令和5年7月4日(火)午前6時30分

- NUTSに障害が発生
- 名古屋港の各コンテナターミナル(飛島北、飛島南、NCB、飛島南側、鍋田)のゲートを閉鎖し、コンテナ搬入・搬出作業を見合せ
- 船舶の荷役については、紙ベースで継続実施

7月6日(木)午前7時30分

- システムの復旧完了

7月6日(木)午後3時以降

- コンテナ搬入・搬出作業再開に向けたデータ入力作業等が完了したコンテナターミナルから、順次コンテナ搬入・搬出作業を開始

搬入・搬出作業開始時間:対象ターミナル
7月6日午後3時00分：飛島ふ頭南側
7月6日午後5時20分：鍋田ふ頭
7月6日午後6時15分：飛島北、飛島南、NCB

7月7日(金)より

- 通常どおり稼働開始

原因

不正プログラム（ランサムウェア※）への感染

※ランサムウェア：感染すると端末等に保存されているデータを暗号化して正常に動作しない状態にする不正プログラム

影響

令和5年7月4日から7月6日までの3日間において、

○荷役スケジュールに影響が生じた船舶
37隻

○搬入・搬出に影響があったコンテナ
約2万本（推計）

コンテナターミナルにおける情報セキュリティ対策等検討委員会　概要

国土交通省

名古屋港のシステム障害に鑑み、コンテナターミナルの運営に関する基幹的な情報システムに必要な情報セキュリティ対策等について整理・検討を行うため、有識者等からなる委員会を設置。

【検討スケジュール】

第1回検討委員会　7月31日
- 名古屋港におけるシステム障害の原因及び対応策の分析
- システムを運用する名古屋港運協会等からのヒアリング
- ヒアリングを踏まえての情報セキュリティ対策に関する議論

第2回検討委員会　9月29日
- 中間取りまとめ①（情報セキュリティ対策、システム障害発生時の対応策）
- サイバーセキュリティ政策及び経済安全保障政策における港湾の位置付けについての議論

第3回検討委員会　11月30日
- 中間取りまとめ②（サイバーセキュリティ政策及び経済安全保障政策における港湾の位置付け）
- 中間取りまとめ①を踏まえての対応

第4回検討委員会　年明け
- 取りまとめ

検討委員会　委員

（有識者）
岩井　博樹　株式会社サイント　代表取締役
小野　憲司　京都大学経営管理大学院　客員教授　＜委員長＞
北尾　辰也　国土交通省最高情報セキュリティアドバイザー
椎木　孝斉　一般社団法人JPCERTコーディネーションセンター　理事
柴崎　隆一　東京大学大学院工学系研究科
　　レジリエンス工学研究センター　准教授

（関係事業者等）
北田　彰　　商船港運株式会社　取締役執行役員
　　(神戸国際コンテナターミナル)
木村　伸児　三菱倉庫株式会社　取締役常務執行役員(港湾運送事業者)
長山　達哉　静岡県交通基盤部　港湾局長(港湾管理者)
名村　悦郎　一般社団法人日本港運協会　理事
人見　伸也　横浜川崎国際港湾株式会社　代表取締役社長
　　(港湾運営会社連絡協議会　会長)

（行政関係者）
紺野　博行　内閣官房内閣サイバーセキュリティセンター　内閣参事官
田島　聖一　国土交通省総合政策局　情報政策課長
稲田　雅裕　国土交通省港湾局長

（オブザーバー）
田中　博　　内閣官房国家安全保障局
　　内閣府政策統括官（経済安全保障担当）付参事官（特定社会基盤役務担当）

中間取りまとめ②に位置付けられた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。

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。