令和5年10月30日
交通政策審議会
第90回港湾分科会
資料6

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の設置と進捗

令和5年10月30日

国土交通省港湾局

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

- 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
- 5つのコンテナターミナルにおける荷役機械、ゲート等と連携している
- 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

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

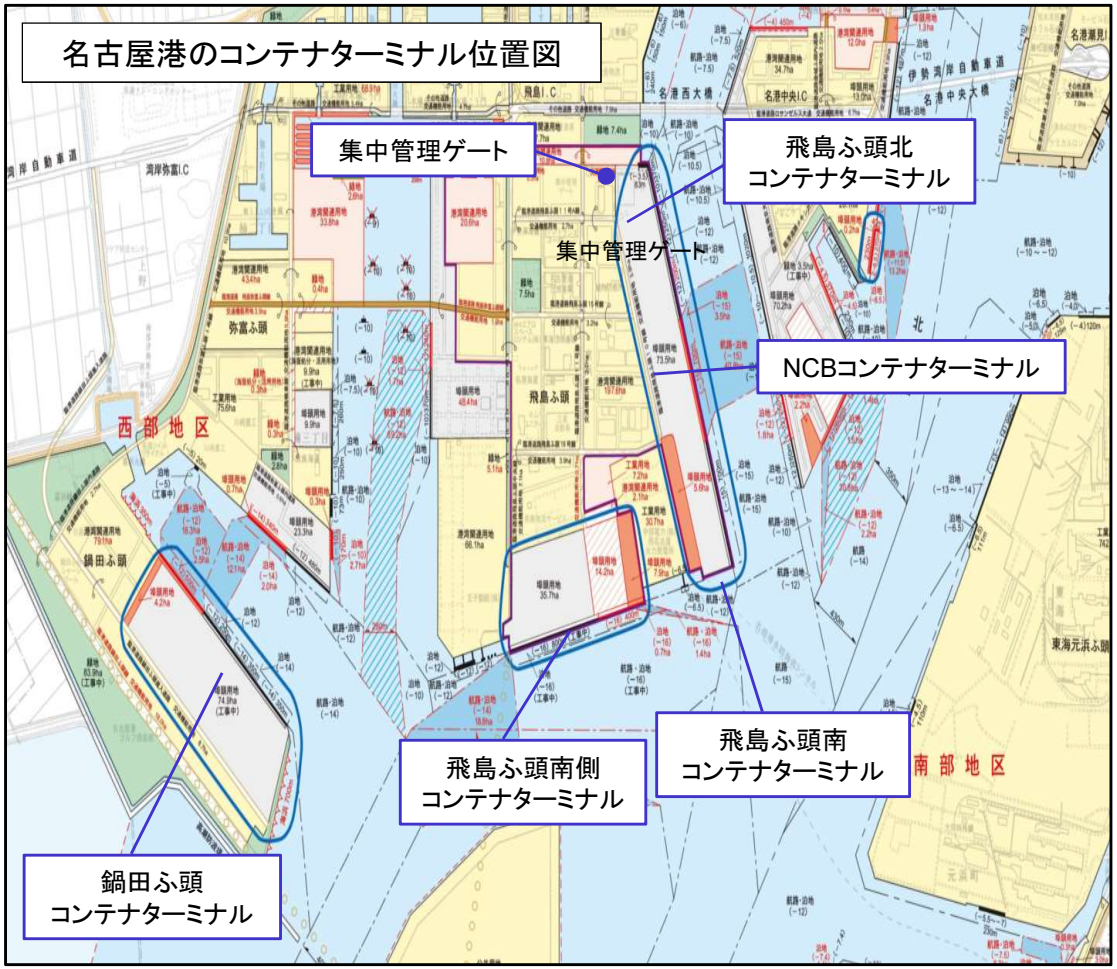
- コンテナ搬入・搬出作業再開に向けたデータ入力作業等が完了したコンテナターミナルから、順次コンテナ搬入・搬出作業を開始

7月7日(金)より

- 通常どおり稼働開始

○障害の原因は不正プログラム（ランサムウェア※）への感染と想定される

※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)

名古屋港コンテナターミナルのシステム障害を受けての対応

国土交通省

有識者委員会の開催

今回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・検討を行う有識者等からなる**「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」**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） （→これらの対策を港湾関係者に共有する説明会を別途開催予定） ・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月頃	・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を踏まえての対応についての議論
第４回検討委員会	年明け	・取りまとめ

注意喚起

○　令和5年7月7日、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、国土交通省の定める「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。

○　令和5年10月2日、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、中間取りまとめ①を周知し、必要な対策を講じるよう注意喚起を実施。

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　中間取りまとめ①

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について（概要）

1．はじめに

中間取りまとめ①は、名古屋港における情報セキュリティ事案を受けて設置された「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」における議論等を踏まえ、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を取りまとめたもの

2．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

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　中間取りまとめ①

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について（概要）

3. 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

○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
○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
○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
○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
○外部委託を行う場合の情報セキュリティの確保　等

4. 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

○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
○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
○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
○情報セキュリティに関する情報の収集
○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
○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

5. 今後の対応

○中間取りまとめ①の周知や説明会の開催により港湾関係者の理解の増進に努める
○コンテナターミナルの重要性やシステム依存度を踏まえた情報セキュリティ対策のレベルについて整理
○サイバーセキュリティ政策や経済安全保障政策における港湾の位置付けについて検討
○諸外国の事例調査、ガイドラインの策定などを通じた、港湾関係者へ有益な情報の提供に努める