中間取りまとめ②　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（案）の概要

国土交通省

資料２－１

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

今回追加

情報セキュリティ対策等の推進のための制度的措置

〇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

〇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

今後の説明会における港湾関係者の意見や、国における制度的措置の具体化に向けた今後の取組等を踏まえ、委員会としても引き続き検討