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（第５回）

議事概要

日時：令和６年11月21日（木）10:30～12:10

場所：中央合同庁舎３号館　８階特別会議室

参加者：別紙参加者名簿のとおり

○　議事次第に沿って、事務局から資料の説明を行うとともに、意見交換を行った。主な意見は以下のとおり。

【議題１　情報セキュリティ対策等に関する制度的措置のフォローアップについて】

○　港湾分野における重要インフラサービス障害の定義を、サイバーセキュリティ基本法に係る港湾の安全ガイドラインにおいて明確化すべきではないか。

○　港湾運送事業法に基づく措置について、事業計画の変更認可申請に際しての課題をおさえておくべき。

【議題２　一般港湾運送事業に係る経済安全保障推進法の基幹インフラ制度の運用開始に向けた指定基準等について】

○　情報セキュリティに関する制度的措置が講じられてきた中で、港湾運送事業者は、新たに経済安全保障推進法に基づく対応を求められている。丁寧な説明を行うなど、事業者の負担軽減に努めて欲しい。

○　港の競争力はハード、ソフトの両輪である。ソフトの中の一つの要素として、情報セキュリティレベルというところに着目をし、それを国として上げていくという大方針については了解した。ロサンゼルス港やロッテルダム港など、情報セキュリティ対策が進んでいる海外の港湾もあると思うが、制度的措置により日本の港湾のセキュリティレベルは国際的に遜色がない水準まで上がるのか、調査を行いながら進めていただきたい。

○　今回の案は、ターミナルオペレーションシステム（以下、「TOS」という。）のみを規制対象とするものとなっているが、例えば、トレーラー搬出入システム等との接続部分についても何らかのセキュリティ対策を担保する必要がある。

○　港湾で使用されているシステムに支障が生じた場合、それが民間事業者の管理するシ

ステムであっても、港湾管理者に問い合わせがなされることが多い。国、港湾管理者、港湾運営会社の果たすべき役割や関係性について、議論をしっかりと進めていただきたい。

○　構成設備の一つをソフトウェアという表現にしているが、他の事業においてはオペレーションシステム、ミドルウェア、アプリケーション等、書き分けている例もある。一般港湾運送事業に係るソフトウェアにはオペレーションシステム、ミドルウェア、アプリケーションが含まれているということだが、規制対象に誤解が生じないように留意すべき。

【議題３　サイバーセキュリティ基本法に係る安全ガイドラインの改定に向けた準備状況について】

○　構成と改定の方向性については、良い取り組みで使いやすいものが出来上がるのではないか。今回のとりまとめ次第では、今後、省内の他部門の安全ガイドラインについても同様の構成とするなども考えとしてはあるのではないか。

○　今回の改定の趣旨は非常によくわかるが、分冊化、特にシステム責任者編とシステム構築・運用者編との切り分け方というのが読み手にとって混乱を招くことのないようにしていただきたい。今後のガイドラインのメンテナンス、また、読み手のわかりやすさなども考えていただきたい。

○　ロサンゼルス港湾局のレジリエンスセンターを視察する機会があったが、自分のことは自分で守るしかないということを感じた。しかし、我々がロサンゼルス港湾局のような体制等とするには財政的にも難しく、セキュリティの専門家もいない中、港湾管理者はこういう体制をとるべきといった提案をしていただきたい。また、事業者がシステムを整えるにあたっての支援についても考えていただきたい。

○　現行のガイドラインはNISCの指針に基づいて体系的に取りまとめられたということもあり、分冊化することによって自分の役割だけをやっていればいいということにならないように配慮した対応が必要である。また、名古屋港の事例を盛り込むにあたっては個別の問題でもあり港湾によってシステムは異なることから記載するにあたっては留意が必要である。

○　推奨事項であるガイドラインと強制要件となる港湾運送事業法とで求める項目が混在する場合は、港湾運送事業者が混乱しないよう棲み分けをしっかりするようお願いしたい。

○　港湾はターミナルだけではなく、税関、出入国審査、検疫などもあり、利用者にとって

はどこのシステムがダウンしても活動できなくなるため、ガイドラインに記載するかは別として、そのような事態の時のことを想定しておくことも必要ではないか。

○　ガイドラインでは、サービス復旧までの時間であるとかKPIを事業者が定めるようになっているが、ターミナル毎にTOSをもっているような場合、それぞれで決めるのは難しい。また、BCPも要件が変わってくるため、ガイドラインでその目標を定めることも必要ではないか。

○　BCPは全ての港湾で作成することが望ましいが、港湾の規模によってTOSへの依存度は異なる。各港湾においてサービス復旧までの時間など、自分たちがどこまで耐えられるのかを評価したうえで、各港湾の実情に応じたBCPを作成する必要があるのではないか。

○　BCPの策定では、復旧の目標時間や目標水準は顧客等を逃がさないという観点から各事業者で定めるのが一般的である。一方で日本では相場感を重視する傾向にあるため、ガイドラインの公表とともに他港の事例のような情報の公開も必要ではないか。

○　港湾におけるサイバーセキュリティに関するBCPの作成や監査については、具体的に何をするべきなのかが難しいと思っているため、ガイドラインでわかりやすく説明する必要があるのではないか。

別紙

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（第5回）
参加者名簿

（有識者）　　（敬称略）

（ご欠席）	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
	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システム創成学専攻　准教授

（関係事業者等）

	鎌田　裕司	名古屋港管理組合　専任副管理者(港湾管理者)
	川村　操	三菱倉庫株式会社　常務執行役員(港湾運送事業者)
	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)
（代理）	吉澤　政克	静岡県交通基盤部港湾局港湾企画課　課長代理（港湾管理者）
	中塚　勝弘	名古屋港運協会　常務理事
	名村　悦郎	一般社団法人日本港運協会　理事
（代理）	髙田　昌行	横浜川崎国際港湾株式会社　代表取締役副社長

（行政関係者）

	佐々木　明彦	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）
	杉本　貴之	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
	中山　泰宏	国土交通省総合政策局　情報政策課長
（欠席）	稲田　雅裕	国土交通省港湾局長