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３回）
議事概要

日時：令和 5 年 11 月 30 日 13:30 ～ 15:00
場所：中央合同庁舎 3 号館　10 階港湾局会議室
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った後、意見交換を行った。主な意見は以下のとおり。

【議題１　中間取りまとめ①に基づく対策の実施状況】
○港湾運送事業者の方から、港湾における情報セキュリティ対策は重要、必要であるというようなお話がある一方、対策を講じるには、人と時間、システム改修のコストが必要になるという声が挙がっている。特に改修コストは多額になることも予想されるので、支援制度を求める声が幾つかあった。予算措置ということになろうかと思うが、その点も検討してほしいと思う。

【議題２　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）について】
○コンテナ以外の、電気、ガス、石油等の専用ターミナルのシステムについては、必要に応じて、ターミナルを所有する事業者において対策が行われているのではないか。
○重要インフラの責務として「サービスを安定的かつ適切に提供」と書かれているが、港湾における「安定的」をどのように定義するのか。留意点として、情報セキュリティ対策の設定条件及び情報セキュリティ対策のレベルをどうするかとあるが、港湾はどこを優先的に評価していくのかがポイントになってくる。できる限りシステムが止まらないように、仮に侵害を受けていても経済を止めないために動かすんだという話であれば、そのための対策を検討していくべきで、その場合には一般的な企業で言われているような予防策中心の情報セキュリティ対策が、多分当てはまらないということになる。他国の重要インフラの攻撃事案を踏まえて、この「安定的」という部分を定義し、何を優先させるかというところを考えていったほうが良い。
○港湾運送事業法に関して、ＴＯＳの所有者には港運事業者、船社、運営会社がいるため、港運事業者に事業計画の対応を求めても、事業者の立場や状況で対応が可能か、あるいは対応に時間がかかるような場合もあるのではないか。事業者の手続等の軽減をお願いしたい。
○港湾運送事業法については、施行規則の改正の年度内施行を目指していきたいと考えている。改正した場合、施行までの間が短いと既存の事業者が対応できないというような事態も懸念されるため、現段階における考え方としては、既存の事業者に対応いただくための猶予期間を設けるつもりでいる。この猶予期間内に事業計画の変更を行っていただくという形で、既存の事業者の負担軽減を考えてまいりたい。
○サイバーセキュリティ基本法における重要インフラへの港湾の位置づけについて、幅広い港湾

関係者において情報セキュリティ対策を着実に講じることが重要と述べられている。港湾分野の関係者には様々な立場の方がいるので、丁寧な説明をお願いしたい。

○関係者として、港湾運送事業者だけではなく、港湾管理者、地方の港運協会といったところも含めて想定している。先日、関係者として想定される方々に対して、行動計画で定められる主な取組について説明させていただいた。引き続き対応をしていきたい。

○経済安全保障推進法では既に１４分野が対象になっており、その大半がサイバーセキュリティ基本法における重要インフラにも位置づけられていることからサイバーセキュリティの重要性等については十分理解されていて、その上で経済安全保障推進法の対象業種になっているのかと思う。その意味で、港湾を対象業種とするか否かについては、慎重な検討をお願いしたい。対象業種となれば規制等がかかって、コスト面への影響も懸念されることから、それらへの支援も検討してもらいたい。

○港湾運送事業者はどちらかというと運用が中心になるかと思う。システム開発を行うベンダーに対してガイドラインを出すなどの検討はしていないのか。

○ベンダーに対する規制権限を持ち合わせていないが、港湾運送事業法を所管しているので、港湾運送事業者に対しての一定の指導は、法令に基づいてできるという形になっている。そこで、今回、港湾運送事業法施行規則を改正し、またサイバーセキュリティに関するガイドラインをつくり、そこできっちりと必要な要件を示していきたい。それによって、結果として、システム開発者の方々においても、その部分に配慮したものをつくっていただくということになってくると考えている。

○ベンダーについても何らかの形でセキュリティ対策の確認ができるようにしていただきたい。例えば制御システムセキュリティの表示でＩＥＣ６２４４３というものがあるが、ベンダーに求める事項については、あえてユーザー側にベンダーが講じるべき事項がきちんと行われているかの確認を求めることで、担保している。そういう形で取り込めるのであれば、より厳密になるのではないか。

○サイバーセキュリティ基本法では、関係機関等という枠組みの中にサイバー関連事業者でベンダー等というのが位置づけられている。サイバーセキュリティ基本法に基づく行動計画の５つの主な対策の中の情報共有体制の強化というところで、例えばどこどこに攻撃がありましたとか、このソフトに脆弱性がありますというような注意喚起が、ＮＩＳＣから重要インフラの所管省庁を通じて重要インフラ事業者に提供されることになる。それを受け取った重要インフラ事業者が、発注している相手に情報提供の必要があるという判断をされれば、その内容についてベンダーに対して提供されるという枠組みになっているため、一定の対応がなされるということになろうかと思う。

○サイバー空間関連事業者自体は、行動計画の中で重要インフラ事業者にとって必要不可欠なＩＴサービスを提供する者として位置づけられ、NISC との情報共有先となっているので、何かインシデントがあった場合は、官民情報共有の枠組みの中に入り得る。重要インフラ事業者が相談相手となる事業者との間で日頃から情報共有体制をつくっていただくことも一つの取組。

○名古屋港の事案では、各ターミナルが統一されたシステムを使用していた。別々のシステムでどれか一つがやられたぐらいだったら、これほど大きなニュースになっていなかったのではな

いか。荷主側の利便性などを考えると、このようにターミナルのシステムを統合していくことは重要なこと。将来的に、ターミナル同士の相互コミュニケーションを阻害してしまうことがないような制度にしていただきたい。

〇ご指摘のとおり、ターミナルのシステムの統合を阻害することがあってはならないと考えている。今回はサイバーセキュリティ事案が発生したが、それをもって過度に恐れることなく、システム化を進めていかなければならない。そのような趣旨はこの取りまとめの中にも入っているし、事務局としてもしっかりとした対応策を示すことで、安心して事業に取り組んでいただけるようにしていきたい。

〇コンテナターミナルのオペレーションシステムはかなり成熟化しており、優劣はそれほどついていない。ユーザー側からすると、共通のシステムができれば非常にやりやすいし、今後システムの監査をするようなことになったときも、一つすれば済む。

〇港湾運送事業者への説明会などの情報については、ホームページ等を通じて共有をいただければありがたい。

〇経済安全保障推進法のスキームについて、設備導入等の契約も対象とある。ターミナルオペレーションシステムは、アプリケーションの部分とネットワークの部分でいろいろシステムが分かれている。例えばネットワークの部分を他社に変えるなどの場合、費用、時間がかかることから、手続が過度に煩雑にならないようにしていただきたい。

〇サイバーセキュリティの問題は日々新しい攻撃が起こって、いろいろ対策、対応が変わってくる。入口のところでの審査で終わりではなく、その後々の運用のところもしっかりやっていただきたい。

以　上

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3回)
参加者名簿

（有識者）　　（敬称略）

	岩井　博樹	株式会社サイント　代表取締役
（委員長）	小野　憲司	京都大学経営管理大学院　客員教授
（ご欠席）	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）

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
西海　重和	国土交通省大臣官房審議官

（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）