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１回）
議事概要

日時：令和５年７月31日 10:00 ～ 12:00
場所：中央合同庁舎３号館　８階特別会議室
参加者：参加者名簿のとおり

○ 小野憲司委員を委員長に選任した後、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、名古屋港運協会、名古屋港管理組合からヒアリングを行い、意見交換を行った。主な意見は以下のとおり。

【名古屋港におけるシステム障害に係る対応等の課題・評価】
○ 今回の対応ではログのバックアップが取れていなかったため、原因の調査に支障が生じている。バックアップを取る期間の延長や、バックアップの取り方をデータが破壊されにくい方式に変更することも有効と思われる。
○ 今後の対応を検討するためにも、原因分析が重要である。システム障害が発生した際の連絡体制についても、警察や保守事業者だけではなく、セキュリティの専門機関にも相談していれば原因特定がスムーズだったと思われる。
○ システム障害の与える影響の大きさを考慮し、早期復旧を優先した判断は素晴らしかった。
○ 港湾をはじめとする物流業界は障害発生時の社会経済へのインパクトが大きい。業界として情報セキュリティのガイドラインを策定した方がよいのではないか。
○ 障害が発生した際の対応手順や原因究明など、業界全体として脅威インテリジェンスの共有体制を整備した方がよいのではないか。
○ 初動で再起動を行ったことは、サイバーセキュリティの観点では推奨されない行為だった。
○ 今は、１～２か月前のセキュリティインシデントの情報が古いと言われる。感度良く業界全体で情報を把握しておくべき。
○ 名古屋港の事案を教訓として、他港で同じような事案が発生しないようにしなければならない。

【全国の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事項】
○ 港毎にシステム依存度は異なっており、その港がどの程度システムに依存しているかによって必要な対策が異なる。
○ 港毎に障害発生時のリスクでランク分けをする等、それぞれ対応を検討する必要がある。
○ 外部接続機器にはセキュリティパッチをしっかり当てる、ID やパスワードは簡素なものでなくセキュリティが高いものを設定する、専用線についてもファイアウォールをしっかり設置する、システムを構成する機器についても適切にパッチを当てる、管理者 ID やパスワードを簡素なものにしないようにする、ログの保全を含めたバックアップを構築するなどが必要な

対策として想定される。

○ インシデント対応の基本的な手順の整理、関係者と連携できる体制を整備しておく必要がある。

○ システムが使用できなくなった場合に備え、マニュアル作業での対応に備えておく必要がある。

○ 今回は各社でシステムに頼らないマニュアル作業の経験があるベテランがいたこともあり、一部作業については対応することができたが、すべての作業をマニュアルで行うことを前提に備えておくことには限界がある。

○ システムは完璧ではないので、障害が起こることに備えたシステムの補強、システムを失ったときにどの程度余力を残せるかという観点は港湾においても大切である。

○ ヒヤリハット事例の共有やベストプラクティス集を作成している業界もある。得られた教訓を業界内で共有しつつ、蓄積していくことで、横のつながりを含めた体制の強化につながると思う。

○ 港湾業界に限らず、同種事案の発生は今後も避けられないと思われる。海外の情報を得るため、コンピューターインシデントレスポンスチーム(CSIRT)の国際会合に業界団体から参加してみるのも有効ではないか。

○ CSIRT を立ち上げるのはハードルが高いということであれば、各港でセキュリティ担当者を任命し、適宜情報共有していくことでセキュリティを高めていくという手はあるかもしれない。

○ 特に資産の把握は重要で、外部との接続において、管理部門が管理できていない機器を勝手に接続されることによるウイルス侵入はよくある。また、保守の際の入口のセキュリティ対策は見落としがち。

○ 本事案をきっかけにＩＴ化・電子化が怖いというイメージを持たれることで、業界全体として逆行することがないようにしてもらいたい。電子化を前提としてしっかりセキュリティ対策を取っていくことが大切。

○ 港毎に個々の事情はあるが、全体の底上げを図るためにも交流などを図りつつ、システムのことを考えていくことが重要。

○ システムの構築については、港運事業者が構築しているケースもあれば、複数事業者が共同で構築するケース、船社が構築するケースなど、港毎に状況が異なっている。

○ 日進月歩で進むリスクに対応するため、対応マニュアル策定の必要性を感じる。また、賠償責任問題に備え、契約においてサイバー攻撃を受けた場合の責任関係を明らかにする必要があると考えている。

○ 事業者が必ずしもサイバーセキュリティに詳しいわけではないので、留意点をまとめたマニュアルのようなものがあればよいと思う。ただ、システムが使用できない場合に、すべてを手作業で対応することは難しいと思われる。

○ 全国 60 港以上にコンテナターミナルがあるが、それぞれ状況が異なるため、統一した対応は難しい。どのようにカテゴリー分けしていくかが重要。

○ たとえば海運業界では、船舶の事故事例等、業界全体でグローバルに情報を共有して再発防止、

改善に取り組んでいる。港湾業界は港毎の情報が共有されていない業界であるので、これを機に情報共有体制が構築されるとよい。

【経済安全保障政策及びサイバーセキュリティ政策に関連する制度について】

○ 物流事業者は公共性が高くセキュリティ対策は重要になってくるが、コンテナターミナルにおいては港湾で統一したシステムが構築されているのはごく一部の港湾に限られており、それ以外の港湾では各社で個別にシステムを構築しているケースが多い点に留意して基準を検討いただきたい。

○ 制度全体での位置づけについては、過去の経緯も考慮して、議論を進める必要がある。

【その他】

○ 原因を究明していくことと、事案の責任の追及は分けて考えなくてはいけない。リスクを最小化していく上で、起こった事案をいかに教訓にしていくかという視点が重要。

○ 今回の事案では、3 日で復旧したということは綱渡りの対応の中で大変よくやっていただいたと思う。大きな港と小さな港で障害が発生した際の影響も異なるので、それに応じた復旧策を検討する必要がある。

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1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
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)
上田　精二	(代理)三菱倉庫株式会社港運事業部　部長(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）

事務局　　国土交通省港湾局 港湾経済課
（協力：総務課、計画課、海岸・防災課）

ヒア対象

藤森　利雄　　名古屋港運協会　会長
市川　和人　　名古屋港運協会　ターミナル部会NUTS電算委員長
黒木　徹　　名古屋港運協会　理事・総務部長
鎌田　裕司　　名古屋港管理組合　専任副管理者