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 2 回）
議事概要

日時：令和 5 年 9 月 29 日 13:30 ～ 16:00
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った後、意見交換を行った。主な意見は以下のとおり。

議事（1）―1【主要港のコンテナターミナルにおける TOS の導入状況等】

○ TOS ごとの取扱貨物量は今回資料にまとめた 36 港の中でもばらつきがあるという理解でよいか。
○ ご認識のとおり。例えば名古屋港のように複数のターミナルで 1 つの TOS を使用している場合は非常に大きな取扱貨物量になる。

議事（1）―2【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）について】

【第 1 章、第 2 章】
＜P.4 2. (3)問題点の抽出と改善点 イ.サーバ機器、システム内のネットワーク機器について＞
○ 1 段落目の「より信頼性の高いセキュリティ対策ソフトを用いるべきである」は、「よりセキュリティレベルの高いセキュリティ対策ソフトを用いるべきである」がより正確な表現だと思われる。
同じく、「一度サイバー攻撃を受けたネットワーク機器は外部からは制御可能な状態となっている可能性も否定できない」の部分に、サイバー攻撃を受けたことが判明したネットワーク機器に関しては、新品への交換を推奨する内容を追記したほうがよいのではないか。
また 2 段落目の「このため、保守用 VPN を通じて物理サーバにランサムウエアが侵入し」の部分について、マルウエアが勝手に拡散したような印象を与えるが、今回は攻撃者がネットワークに侵入したという形なので、「攻撃者」に改めたほうがよいのではないか。
同じ箇所について、今回の侵入経路は VPN 経由である可能性を想定した記載になっているが、現時点でまだ VPN 経由の可能性が高いとまでと断定できる状況ではなく、他の可能性も想定される。今後調査、事実が明らかになるに従い、最終取りまとめでは修正される可能性があるということは御認識いただきたい。
○ 今の議論に関連して、現時点で原因が明確になっていない中で、港湾全体の安全、サイバーセキュリティ対策の強化を総合的に考えるにあたり、今回の事案の原因にあまり拘りすぎずに対策を一般論化して考えていくことも重要である。

【第 3 章】

＜P.6 3. (3)外部との接続　ア.VPN＞

○　VPN にフォーカスした記載になっているが、侵入経路はまだ判明していないので、昨今のサイバー情勢を鑑みて、ネットワーク機器全般を広く読めるようにしたほうがよい。

○　該当箇所を「VPN ルータ等のネットワーク機器」に改める。

＜P.7 3. (2)外部との接続　ア.VPN＞

＜P.7 3. (3)サーバ機器、システム内のネットワーク機器＞

＜P.8 3. (4)バックアップ＞

○　第 1 回委員会ではバックアップと並んでログ取得の重要性は非常に強く指摘があったところ。ログついては既に数か所で記載されているものの、ログ取得の重要性はネットワーク機器関連だけではなく、ホスト等の計算機等やサーバ等でも非常に重要。また、ログのバックアップを取得するだけではなく、ログが常時取られていること、定期的に記録されていることが重要であるため、ログ取得の重要性について更に強調して記載したほうがよい。

○　「3. (3)サーバ機器、システム内のネットワーク機器」でもログの取得について追記する。

＜P.8 3. (3)サーバ機器、システム内のネットワーク機器＞

○　TOS を構築する際に IaaS 型クラウドサービスを利用している場合、IaaS 独特の仕様としてアクセスキー(識別コード)で認証を行うが、多要素認証等が使用できないため、アクセスキーの流出により侵害の原因になっているケースがある。アクセスキーの取扱いに十分注意することが重要等の記載を追加いただきたい。

○　3. (2)及び(3)に「識別コードについて、安全な配布方法と運用手順を定めること。」と追記する。

＜P.8 3. (4)バックアップ＞

○　「バックアップは TOS と同時にサイバー攻撃を受けることがない場所に保存する」とあるが、サイバー攻撃を受けることがない場所というのは、どういう想定か。所謂エアギャップに関連することか。

○　直接運用しているサーバ内等ではなく、ネットワークから切り離されたシステムやディスク等の物理ファイルでの保存を想定している。「現用のシステムとは切り離した場所に保存する」との表現に改める。

【第 4 章】

＜P.10 4. (2)情報連絡体制　イ．専門組織への情報共有＞

○　今回の名古屋港の事案の初動時にサイバーセキュリティの専門家の意見を聞く場面がなかった点は非常に気になっており、専門組織への情報共有が記載されたことは重要であると認識している。早い段階で専門組織に相談し、然るべき技術的なアドバイスを受けることは警察等への報告と並列して非常に重要となる。また、原因特定にあたっても、事業者に直接関わるベンダー等が調査した場合、客観的な判断が難しい部分もあるため、中立的な専門機関にセカン

ドオピニオン的な相談をすることは非常に重要と認識している。

＜P.9 4. (1)組織・体制の確立＞

○ CISO の役割として、「情報セキュリティ対策を推進する上での最終決定権及び責任を持つこと」とされているが、一例としてどういった役職の方が CISO を担うことになるか。

○ 具体的な役職を想定しているものではなく、「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」と表現を合わせている。事業者によっては社長が担うケースもあると思われるが、名古屋港のように複数事業者で TOS を運用している場合には代表事業者の執行役員クラス等、責任を負うことができる者が担うことが想定される。

＜P.10 4. (2)情報連絡体制 エ. 対外的な情報発信＞

○ 近年、ランサムウエア事案においても攻撃者側から攻撃を行ったことを公表するケースが出てきており、対外的な情報発信についても狭義の関係者に限らず広く発信・公表を行う必要性について言及してはどうか。

○ 「TOS の利用者等に対して、提供しているサービスの状況、復旧見込み等について適切な情報提供を行うこと」を「TOS の利用者等の関係者に対して、提供しているサービスの状況、復旧見込み等について適切な情報提供・公表を行うこと」と改める。

【第 5 章】

＜P.12 5.＞

○ 各港におけるセキュリティ対策レベルの底上げが非常に重要だと考えており、「本中間取りまとめの周知、説明会の開催などを通じ港湾関係者の理解の増進に努める」とのことで、港湾管理者をはじめ、関係者へしっかりと周知いただきたい。また最終とりまとめに向けて、各港の事情も汲んだうえで、レベルに応じた必要な情報セキュリティ対策を検討いただきたい。

○ TOS 導入ターミナルが３６か所あるという調査結果からもわかるように、それだけシステムが港毎、事業者毎により異なっており、必要な対策のレベル感はそれぞれ異なる点は御理解いただきたい。

○ 本中間取りまとめの第３章、第４章は「推奨」される取組をまとめたものと理解している。事業者毎に対応できる対策は異なるため、しっかりと関係者に理解を得るようにしていただきたい。

＜P.12 4. (5) 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＞

○ 情報セキュリティ意識の向上と教育にあたっては、特に訓練による意識・能力の向上が重要。一般的なシステム障害からの復旧でも、実際にやってみると様々な発見があり効果的である。

○ インシデントに特化した形ではあるが、4. (1) で対応訓練を記載している。セキュリティ意識の底上げ等も意図して、該当箇所を「情報セキュリティに係る教育・訓練」と改める。

【その他】

○ 今回、取りまとめるにあたり様々な御意見を伺う中で、事業者からは、セキュリティ対策の必要性は理解する反面、投資できるコストには限界があるという点と、障害発生時に原因究明と事業の再開がトレードオフの関係になっており、原因究明のために港湾をストップすることで却って物流の混乱を引き起こしてしまう点などについて懸念の声があった。情報セキュリティが疎かになっていいわけではないが、御意見として紹介させていただく。

○ 今回の名古屋港の事案のようなサイバーセキュリティインシデントは、今後も起こり得るという認識を持ち、備えておくことが重要。また、事業再開と原因究明のトレードオフの問題については、原因究明を専門家に任せることで、自分たちは復旧に向けた作業を行うこともできるはず。セキュリティ対策に対してマイナスイメージを持つのではなく、様々な対応策がある中で、専門組織等の活用も検討していければよいと思う。

○ 各委員から御指摘のあった点については、事務局から修正版として再度発言者に確認の後、最終版をとりまとめさせていただく。

議事（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づけについて】

＜全体に係る意見＞

○ 港湾荷役に用いられるシステムにはコンテナ船以外にもフェリー、ＲＯＲＯ船、バルク船等、様々な船種に対応した機能があるが、マニュアルでも対応できる部分もあるし、システムのカバレッジがまだまだ低い。
また、コンテナターミナルの TOS の周辺システムとして、ターミナルの出入管理や、ＣＩＱに係る部分、NACCS 等、港湾分野のデジタル化は進んできている部分はあるが、まだ発展途上といえる。そのため、今回はコンテナターミナルの TOS に集中して検討を進めていくと理解した。

○ 港湾や空港の物流に深く関わる分野は、昔からテロの対象で、広い意味で脅威、インテリジェンスを重視しなければならない分野だと理解している。その中の一つに情報セキュリティがあると捉えたときに、そういった脅威情報や、ソフトウエアの脆弱性情報の収集が日々行われるものであると思うが、脆弱性対策の状況の確認は定期的なものでよいのか。情報を収集してキャッチしたら、随時確認していくべきであり、それが広い意味で、国家安全保障の観点で、現状を捉えた内容になるのではないか。

○ 中間取りまとめ①はとても有効だと認識している。しかし、個々の会社の対応は進んでも、所有者と運用者が違っているという問題もあり、個々の会社のシステムと同様に共有システムを運用するのは、実際には難しいと思う。個々の会社は、サイバーセキュリティについてはレベルを上げてきていると思うが、共有システムでは隙間があるのではないかと思う。（

＜資料 2-5 P.2（２）外部との接続＞

○ 現行の物流ガイドラインや、世の中のガイドライン的なものに関して、幾つか抜けている点がある。その一つは、今回の中間取りまとめ①のＰ７のウ．にある、いわゆる閉域網、インターネットに介さない、専用線やＮＡＴ経由のところで、今までは相手方を信用して専用線はあま

り対策しなくてよいという考え方だったが、インターネットだけではなく、専用線もファイアウォールを設置して、必要な通信だけに絞る等の対策をするのが今の考え方である。中間取りまとめ①では、その点も反映されている。

○ 従前のガイドラインでは、防御型の対策は多いが、検知型の対策が少ない。万一破られた場合や、不審な動きがあったときに、どこまで対応するかという論点はあるが、検知型の対策を加えていき、もし、何か不審な動きがあったときに早期に検知できるという事が望ましい。中間取りまとめ①では、専用線に対して防御型の対策が書いてある。

＜資料 2-5 P.3（４）バックアップ＞

○ 資料２－５のＰ３の（４）バックアップについて、恐らく物流ガイドラインもそうだが、従前のガイドラインだと、災害やシステム障害のバックアップのことが記載されていることが多いが、サイバー攻撃によっても破壊されない、生き残るようなバックアップが求められる。中間取りまとめ①では、そのような書き方になっている。

＜資料 2-5 P.7（７）脆弱性や設定不備の定期検査＞

○ 従前は、防御型の対策が多いが、中間取りまとめ①の P12 の（７）脆弱性や設定不備の定期検査で、定期的に設定不備を見つけ出すという事が書かれている。しかし、「脆弱性対策の状況を定期的に確認すること。」という書きぶりで、トーンが弱く、一昔前の書き方になっていると思う。最近は、外部と接続しているものについては１か月程度のサイクルで、設定不備がないか見つけ出すという世の中の流れがある。資料２－５の P7 の（７）脆弱性や設定不備の定期検査の現行制度のところも、若干、一昔前の書き方になっているように見えるため、新しくガイドラインを加える際には書き方を考えていただきたいと思う。

○ 資料２－５の P7 の（７）脆弱性や設定不備の定期検査の現行制度のところは、脆弱性しか書いていない。特に、弱いパスワードがそのまま使われていることや、不要なポートが開いている、といった点がポイントになってくるため、中間取りまとめ①の P12 の（７）脆弱性や設定不備の定期検査に、設定不備の項目を入れているし、そういった点を加えると、今回の事案を踏まえた良いガイドラインになるのではないか。

＜ガイドライン策定に係る意見＞

○ ガイドラインの世界も年々ブラッシュアップされているため、遅れを取らないように、世の中のガイドラインよりも先を見越して、最先端の状況を踏まえた対応になるようにガイドラインを作成していっていただければと思う。中間取りまとめ①はそういったことも踏まえて作成している。

○ 既にある、国際的なガイドラインをレビューして活用するのも一つの方法。中間取りまとめ①のＰ１に、参考文献として、ＩＡＰＨの Cybersecurity Guidelines for Ports and Port Facilities Version １.０を取り上げているが、これが既存のものとして一つのリファレンスになるのではないか。

○ 別の視点として、海事方面にも動きがある。船舶も含めた大きく広い海事という枠の中で、港

の役割が検討されてきていると思う。ＩＭＯでは、情報セキュリティガイドラインを改定していこうという動きもあるというような話も聞いており、その中での港湾の役割が新たに関係してくると思う。海事と港湾が融合した動きが今後出てくると思われるため、そういう視点も入れていただくと良い。

○ 日本の港湾のセキュリティレベルをしっかりと確保し、やはり世界の最先端であってほしい。少なくとも世界の水準から見て、遅れを取ってはいけない。例えば、ＩＡＰＨがどういうガイドラインの中身になっているのか、ＩＭＯの動きはどうなのか、そういったことをリファレンスすることが必要。

○ これまでコンテナターミナルで行ってきた、あるいは検討されてきたセキュリティ対策の内容を、RORO 等の他の全体の議論に置き換えることができるのか疑問がある。RORO などの現状も踏まえて、過剰な書きぶりにならないように、適切な書きぶりになると良い。

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2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
	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
（ご欠席）	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)
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
（代理）	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）