資料4－2

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
取りまとめ（案）

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

１．はじめに

2017 年 6 月に世界的な海運会社である A.P. モラー・マースクの 17 のコンテナターミナルがサイバー攻撃を受け、2020 年 5 月にはイランのシャヒード・ラジャイ港がサイバー攻撃を受ける等[1]、近時港湾施設へのサイバー攻撃が相次いでいる。我が国においても例外ではなく、2023 年 7 月 4 日には名古屋港の 5 つのコンテナターミナル及び集中管理ゲートで運用されている名古屋港統一ターミナルシステム（以下「NUTS」という。）が、我が国の港湾施設にとって初めてとなる大規模なサイバー攻撃を受けて停止し、約 3 日間にわたり名古屋港のコンテナの搬入・搬出が止まる等物流に大きな影響を及ぼすこととなった。

今般の名古屋港における情報セキュリティ事案を踏まえ、国土交通省では当該事案の原因究明を行うとともに、同種事案の再発防止に向け、必要な情報セキュリティ対策や関連法令における港湾の位置付け等について整理・検討を行うため、「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」（以下「委員会」という。）を設置した。

7 月 31 日には第 1 回委員会を開催し、NUTS を運用する名古屋港運協会及び港湾管理者たる名古屋港管理組合からのヒアリングを実施するとともに、コンテナターミナルにおける情報セキュリティ対策に関する議論を実施した。

9 月 29 日には第 2 回委員会を開催し、第 1 回委員会における議論及びその後の調査を踏まえるとともに、「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（第 4 版）」（平成 31 年 3 月 29 日改訂　国土交通省）を参考に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について「中間取りまとめ①」として取りまとめた。

11 月 30 日には第 3 回委員会を開催し、上記に加え、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「中間取りまとめ②」として取りまとめた。

以上の検討の経緯を踏まえ、今般、本委員会としての取りまとめを行うものである。

---

[1] p.p.21-22, IAPH – Cybersecurity Guidelines for Ports and Port Facilities Version 1.0 - Published 2 July 2021, https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

継続して港湾の利便性向上を図るためには、今回の名古屋港における事案を過度におそれて港湾における IT 化、DX 化の流れを止めるのではなく、適切な情報セキュリティ対策を講じることでこれらを推進していく必要がある。そのためにも、本取りまとめが活用されることを強く希望する。また、国において、港湾関係者の理解の増進に努めるとともに、制度的措置の具体化に取組むことを期待する。

なお、本取りまとめの目的は特定の者の責任を追及することにあるのではなく、今回の事案を多くの関係者と共有し、我が国のコンテナターミナルの情報セキュリティ対策を強化することにあることを付言する。

２．名古屋港事案の検証

（１）事案の概要及び対応状況

名古屋港運協会からのヒアリングを通じ、以下の事案の概要及び対応状況を確認した。

【7 月 4 日（火）】

06:30 頃　NUTS システムの作動が停止したことを確認

07:15 頃　状況確認後、システム保守会社及びシステム開発会社へ調査を依頼

07:30 頃　システム専用のプリンターからランサムウェア[2]の脅迫文書が印刷される

08:15 頃　サーバが再起動できないことが判明

09:00 頃　愛知県警察本部サイバー攻撃対策隊（以下「愛知県警」という。）に連絡、状況確認後、ランサムウェアに感染した可能性があるとの見解が示される

10:30 頃　港湾での物流を早期に再開させるため、システム復旧を優先するよう判断、復旧作業開始

14:00 頃　物理サーバ基盤及び全仮想サーバが暗号化されていることが判明

18:00 頃　ランサムウェアに感染の可能性が高まったことから、愛知県警と今後の対応について協議を行う

【7 月 5 日（水）】

02:00 頃　物理サーバ基盤全 8 台が復旧、仮想サーバ（45 台）の復元作業を開始

12:00 頃　名古屋港運協会より、今回のシステム障害の原因がランサムウェアへの感染であることが判明したこと等をプレス発表

12:00 頃　仮想サーバの復元完了、ウイルスチェックを開始

21:00 頃　復元した仮想サーバからウイルスが検知され、ウイルス駆除の必要があると判

[2] 感染すると端末等に保存されているデータを暗号化して、正常に動作しない状態にする不正プログラム。

断

【7 月 6 日（木)】

02:00 頃　ウイルスチェック終了、最終的にトロイの木馬 120 個マルウェア 4 個その他 8 件のウイルスを検知、ウイルス駆除を開始

07:15 頃　ウイルス駆除終了、バックアップデータから CS[3]/CTMS[4]等単体では復元が完了したが、CS/CTMS の連携に障害が発生

14:15 頃　連携障害が解消、データと実在庫情報の整合性の確認を開始
準備が整ったターミナルより順次作業を再開する

15:00　飛島ふ頭南側コンテナターミナル(TCB) 作業再開

16:30　鍋田ふ頭コンテナターミナル(NUCT) バンプール（空コンテナ）作業再開

17:00　NUTS WEB 稼働再開

17:20　鍋田ふ頭コンテナターミナル(NUCT) 全ての作業再開

18:15　NCB、飛島ふ頭北、飛島ふ頭南コンテナターミナル作業再開

また、今般のシステム障害による影響としては、荷役スケジュールに影響が生じた船舶37隻(NUTSが停止したことによりマニュアル作業で荷役を行ったものの、最大 24 時間程度の遅延が発生した。)、搬入・搬出に影響があったコンテナ約 2 万本（推計）の他、トヨタ自動車の愛知県と岐阜県にある 4 つの拠点の稼働停止、アパレルメーカーにおける衣類の入荷遅延等の経済活動への影響も報道[5]されている。

（2）感染経路

ランサムウェアの感染経路として考えられているのは、①指定ユーザのみ利用可能な仮想専用線たる VPN[6]機器からの侵入、②外部記憶媒体である USB メモリからの持ち込み、③NUTS と港湾運送事業者間とのネットワーク連携で運用している NAT[7]変換による NUTS への接続からの侵入の 3 点である。

---

[3] Control System の略。NUTS の基本情報を統合管理する基幹システム。

[4] Container Terminal Management System の略。CS とデータ連携しターミナル運営を行うためのトータルパッケージシステム。

[5] NHK「名古屋港システム障害 ターミナルすべてで運用再開 物流混乱も」2023 年 7 月 6 日 19 時 18 分、
https://www3.nhk.or.jp/news/html/20230706/k10014120421000.html

[6] Virtual Private Network（仮想プライベートネットワーク）の頭文字を取った略語で、インターネット接続とオンラインのプライバシーを保護する仕組み。VPN 接続は、仮想的な専用線を構築することで確立される。

[7] Network Address Translation（ネットワークアドレス変換）の頭文字を取った略語で、グローバル IP アドレスからプライベート IP アドレスを紐付けて変換する技術。

サーバ内のデータが全てランサムウェアにより暗号化されておりログを解析することが困難なため、感染経路を断定することはできないものの、今般の事象においては、8 台ある物理サーバが全て暗号化されシステムが起動しなくなっていることから、アプリケーション経由ではなく、サーバ部への直接的な攻撃が行われた可能性が高く、VPN 機器からの侵入が行われたものと見ることが適切である。

現に、NUTS の保守用 VPN には緊急時に即時に対応するため IP アドレスに制限をかけておらず、ID とパスワードさえ合致すればインターネット上で誰からでもアクセス可能な状態にあったこと、VPN 機器及び物理サーバに関して数か月前から脆弱性が公表されていたものの、これら脆弱性への対応が未対応であったことが確認されている。

ただし、保守用 VPN で未対応であった脆弱性については、現状いくつかの標的型攻撃のみでの悪用が知られているのみであり、名古屋港の事案で攻撃に使用されたランサムウェアによる攻撃においてこの脆弱性が悪用されたケースは知られておらず、保守用 VPN 経由の侵入であった場合も脆弱性の悪用以外の方法で侵入された可能性が高い。たとえば、攻撃者による保守用 ID とパスワードの不正取得や推測による攻撃によるものが考えられるが、これについても特定はできていない。このため、保守用 VPN を通じて物理サーバに攻撃者が侵入し、サーバ情報が暗号化されたものと考えられる一方で、VPN 経由以外での侵害の可能性についても否定することはできない。なお、原因については現時点で幅広に捉えておくべきだが、これによりその他の対策に大きく影響するものではない。

（3）問題点の抽出と改善点

今般の事案における問題点とその改善点として以下の点を挙げることができる。

ア．外部との接続について

・今般の事案における大きな問題点の１つは、保守作業に利用する外部接続部分のセキュリティ対策が見落とされていたことである。一般ユーザ向けのセキュリティ対策に目が行きがちであるが、保守等いわば身内に潜むリスクにも目を向けセキュリティ対策を講じる必要がある。

・VPN 機器のログのバックアップが取得できていなかったこと。今回のケースのようにシステム内の情報が暗号化されてしまった場合に、入口である VPN 機器のログの解析は感染経路等の特定に役立つものであり、可能な限り VPN 機器のログのバックアップも取得しておくべきである。

イ．サーバ機器、システム内のネットワーク機器について

・ウイルス対策として基幹 OS 付属のセキュリティ対策ソフトのみを活用していたこと。基幹 OS 付属のセキュリティ対策ソフトは最低限の機能を有するものであり、NUTS に求められるセキュリティレベルとしては不十分なものであったと考

えられる。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。

・ネットワーク機器が踏み台になっていた可能性があること。システムのみならず、ネットワーク機器もサイバー攻撃の対象となりうるものであり、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制御可能な状態となっている可能性も否定できない。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、新品と交換する等サイバー攻撃を受けた状態のままでの継続使用は避けることが望ましい。

ウ．バックアップについて

・原因を分析するためのログ（システムログ、アクセスログ）が暗号化被害のため取得できなかったこと。原因を分析するためのログについても、定期的なバックアップの対象とすべきである。

・原因調査、システム復旧の両方の面で、バックアップが直近 3 日分のみでは不足していたこと。今般の事案ではバックアップデータ中からもウイルスが見つかっていることから、ウイルスに感染する前のクリーンな状態のバックアップデータを保持するべく、システムプログラム等の更新頻度が低く必要性が高いデータについてはより長期間のバックアップを取ることを検討すべきである。一方で、コンテナ情報等の動的データについては、バックアップについてもできるだけ最新を維持できるよう取得頻度を高める等の工夫が必要である。

・NUTS の本番環境のみをバックアップの対象として、開発環境、評価環境をバックアップの対象としていなかったこと。バックアップ容量及びコストの関係で、バックアップの対象が限定的であったことで却って復旧時間及び復旧費用を増大させることとなった。可能な限り、開発環境、評価環境についてもバックアップの対象に含めるべきである。

エ．障害対応体制について

・システム障害発生時の対応手順が事前に整備されていなかったこと。災害用の事業継続計画（以下「BCP」という。）は事前に整備されていたものの、システム障害発生時の BCP が事前に整備されていなかった。サイバー攻撃も対象としたシステム障害発生時の BCP を整備すべきである。

・インシデントの調査や原因究明を行うにあたって証拠として必要なログ、データに関して、暗号化によってアクセスができなくなったデータに加えて、復旧対応によって失われたログやデータが存在する。証拠保全を考慮したインシデント対応手順を整備することが望ましい。

・初動対応時にサイバーセキュリティ専門家の意見を聞く場面がなかったこと。システム障害の状況を確認後、名古屋港運協会はシステム保守会社及びシステム開発会社へ連絡を入れているが、サイバーセキュリティ専門家への相談は行われて

いない。システム保守会社やシステム開発会社は当該システムの専門家ではあっても、サイバーセキュリティの専門家ではない。原因究明やシステム復旧後のシステムのセキュリティ対策状況が適切であるかどうか確認するためにも、情報セキュリティ事案発生時にサイバーセキュリティ専門家と直ちに相談できるよう、日頃から関係を構築しておくことが望ましい。また、原因特定においても初動対応と同様に、サイバーセキュリティ専門家にセカンドオピニオン的な相談ができる体制が望ましい。

・情報セキュリティ事案発生時における港湾管理者と港運協会の連携が重要である。港湾管理者は、非常事態下においてどのような役割を果たすべきか、日頃から検討を行うとともに役割分担等について港運協会と事前に調整しておくことが望ましい。

・セキュリティの観点で、システムの健全性をログ等により定期的に確認するとともに、異常が検知された場合には、適切に対応ができる体制を構築しておくことが望ましい。

オ. 運用再開時の情報セキュリティ対策状況の確認

・感染経路を踏まえた情報システムの健全性の確認・評価が十分ではなかった。システムの運用を再開する前に、適切な情報セキュリティ対策が取られている状態であるかどうかの確認・評価を行う必要がある。

（4）グッドプラクティス

今回の事案では、対応に問題があった点がある一方、対応として評価できる点もある。特に以下の項目は、他のコンテナターミナルにおいても参考としてほしい。

・日頃より情報セキュリティ研修等の場を通じて愛知県警と名古屋港運協会との関係が構築できていたこと。これにより、事案発生時の相談、対応がスムーズになされた。

・事案発生後早い段階で、名古屋港運協会幹部の指示の下、同ターミナル部会が招集され、復旧までの間、事実上の意思決定機関として機能したこと。特に、復旧を最優先するとの判断により、結果として事案発生から丸2日半という短期間で復旧が図られた。

・マニュアル作業により船舶との間の荷役が継続されたこと。遅延が生じたとは言え、紙で印刷した作業内容に基づき荷役が継続されたことで、名古屋港をスキップする船舶はなかったとされている。なお、今回はシステム化がされる以前のマニュアル作業の経験者がいたことにより対応が可能であったものであり、全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は非現実的であるとの指摘もある。

３．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

コンテナターミナルにおけるコンテナの積卸し作業、搬入・搬出等を一元的に管理するターミナルオペレーションシステム（以下「TOS」という。）に必要な情報セキュリティ対策として、以下の取組を推奨する。

（１）資産の把握

TOS がコンピュータウイルスへの感染や外部からの不正侵入等のサイバー攻撃を受けた際の侵入経路やシステムに与える影響の範囲等の情報セキュリティリスクを推定し対策を検討するために、システムの機器構成、ネットワーク構成、外部との接続状況、システム外の機器（未管理機器）の接続状況等を把握しておくこと。これらの情報は、実際にサイバー攻撃を受けた際の侵入経路の特定等にも資する。

（２）外部との接続

TOS がサイバー攻撃を受けた際のシステムへの侵入口となり得るのは、外部との接続部分である。本項では、TOS で主に用いられている外部接続手段を対象にその対策を示す。

ア．VPN ルータ等のネットワーク機器

港湾運送事業者や TOS のシステム保守会社及びシステム開発会社が外部（自社や自宅等）から TOS に接続する際に利用するものである。

予め許可された者のみがシステムへの接続が可能となるよう、以下の措置を執ること。

- 接続元の IP アドレスを指定することで接続元を限定、明確化する。
- 知識情報（パスワード等、利用者本人のみが知り得る情報）、所有情報（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）、生体情報（指紋や静脈等、本人の生体的な特徴）のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの（12 文字以上、大小英文字＋数字＋記号を推奨）とする。
- 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。
- アカウントロック機能を実装することが望ましい。
- 不正ログイン試行を検知する機能（通常とは異なる IP アドレスからシステムへアクセスがあった際にメールで通知等）を実装することが望ましい。

また、VPN ルータ等のネットワーク機器の脆弱性がサイバー攻撃の対象となり得ることから、ネットワーク機器について以下の措置を執ること。

- ネットワーク機器上で利用しているソフトウェアの情報を定期的に確認し、確実に更新する。
- ネットワーク機器の通信記録等のログを定期的に取得するとともに、シス

テム外にバックアップを保存する。

・　サイバー攻撃を受けた場合、ネットワーク機器が踏み台となっている恐れがあることから、新品と交換する。

イ．外部記憶媒体（USB メモリ等）

荷役を行う船舶と TOS の間でコンテナの情報を共有する際等に USB メモリを使用する例が見受けられる。

情報セキュリティの観点からは、USB メモリ等の外部記憶媒体の利用はできる限り控えることが望ましいが、止むを得ず利用する場合には、事前に TOS とは切り離された端末によりウイルスチェックを確実に行い、異常がないことを確認してから使用すること。

ウ．専用線、NAT

TOS は一部の外部システムとは専用線により接続されている。また、港湾運送事業者から TOS に接続する際に NAT を使用する例も存在する。これらは比較的安全な接続方法ではあるが、そうであっても万が一の事態に備えファイアウォールを設置する等の措置を執ることが望ましい。

（3）サーバ機器、システム内のネットワーク機器

TOS がサイバー攻撃を受けた際のシステムへの影響を最小化するため、サーバ機器及びシステム内のネットワーク機器の対策を以下に示す。

・　サーバ機器に対して基幹 OS の付属品以外のセキュリティ対策ソフトを導入し、ウイルスパターンを常時最新のものに更新する。

・　サーバ機器及びネットワーク機器のログを定期的に取得するとともに、システム外にバックアップを保存する。

・　サーバ機器及びネットワーク機器上で利用しているソフトウェアの情報を定期的に確認し、確実に更新する。

・　管理者の認証に当たっては、知識情報（パスワード等、利用者本人のみが知り得る情報）、所有情報（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）、生体情報（指紋や静脈等、本人の生体的な特徴）のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの（12 文字以上、大小英文字＋数字＋記号を推奨）とする。

・　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。

（4）バックアップ

TOS がサイバー攻撃を受けた際の業務継続にあたり、必要に応じてバックアップシステム（予備系統）を用意しておくこと。また、早期復旧や原因究明のため、以

下の点に留意してTOSのバックアップを取ること。

- バックアップを取るべき主な対象として、システムプログラム（開発環境、評価環境を含む)、コンテナ情報等の動的データ、システムログ等が挙げられる。
- 最後にバックアップを取得した時間から情報セキュリティ事案発生時までの更新情報が失われる可能性を考慮し、バックアップ対象ごとにバックアップの取得頻度を設定すること。
- コンピュータウイルスの潜伏期間を考慮し、バックアップは直近のもののみではなく、数週間前のものを含めて複数保存しておくこと。
- バックアップは現用のシステムとは切り離した場所に保存すること。

（5）クラウド利用時の対策

クラウドサービスを利用して TOS の機能を実現している場合においても、上記（1）～（4）の対策を実施するとともに、以下を例とするセキュリティ要件をクラウドサービスに求め、契約内容にも含めること。

- アクセスログ等の証跡の保存及び提供
- 委託先による情報の管理・保管の実施内容の確認
- 脆弱性対策の実施内容の確認
- 情報の確実な削除・廃棄　等

（6）TOSと連携している外部機器への影響

TOS と連携している外部機器が存在する場合、TOS から当該外部機器の制御権を取得できるかどうか確認の上、取得できる場合は必要な対策を執ること。

（7）外部委託を行う場合の情報セキュリティの確保

TOSの開発・保守等を外部委託する際は、委託先の選定手続、選定基準及び委託先が具備すべき要件を予め整備の上、これらに基づき委託先を選定すること。また、委託先に請け負わせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。)、システム障害に対する対処手順及び情報セキュリティ対策の履行が不十分である場合の対処手順を含む契約を取り交わすこと。

4．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

TOS に必要な情報セキュリティ対策を実施する体制として、以下の取組を推奨する。

（1）組織・体制の確立

ア．最高情報セキュリティ責任者等の指定

情報セキュリティ対策の推進の責任者（役員クラスが相当）として最高情報セキ

ュリティ責任者（CISO）を指定すること。CISO は、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。

また、情報セキュリティ対策の検討及び実施並びに情報セキュリティ事案発生時における対応を主導する情報セキュリティ担当者を指定すること。情報セキュリティ担当者の役割例を以下に示す。情報セキュリティ担当者は、複数名にて役割分担しても構わない。

- 脅威情報等の収集及び関係主体との情報共有
- セキュリティインシデントの管理（CSIRT 等）
- 事業継続計画（BCP）等の実行
- 情報セキュリティ対策の取組全般に対する内部監査
- TOS のシステム開発会社やシステム保守会社における情報セキュリティ対策取組の管理
- セキュリティ人材の職能要件の管理及び教育・研修
- 情報システム（ネットワークを含む）の運用
- 各資産（情報システム、ソフトウェア、情報等）の管理
- 物理的セキュリティが要求される施設の管理
- 制御システム等が運用される環境保有時には制御システム等関連部門の担当

イ．セキュリティインシデント対応手順の策定

サイバー攻撃等のセキュリティインシデントが発生した場合に備え、証拠保全、被害の拡大防止、システム障害復旧、原因調査等に必要な報告や対応の手順等を予め整理しておくこと。なお、ランサムウェアによる攻撃を受けた場合は、攻撃元の要求に応じて金銭の支払いを行うことは厳に慎むこと。

ウ．セキュリティインシデント対応訓練の実施

サイバー攻撃等のセキュリティインシデントが発生した場合に適切な対応が取れるよう、前項の手順の確認等を行う訓練を定期的に実施すること。

エ．セキュリティ運用・監視の実施

システム機器のログ等を定期的に確認することによりシステムのセキュリティの状況を定期的に把握するとともに、異常が検知された場合には早い段階で対応し、可能な限り重大なインシデントに発展することを未然に防ぐこと。

（2）情報連絡体制

ア．自組織内の情報共有

セキュリティインシデントが発生した場合、情報セキュリティ対策の観点から CISO 及び各情報セキュリティ担当者間で速やかに情報共有を行うとともに、業務継続の判断等を行う経営層に対しても速やかに情報共有を行うこと。

イ．専門組織への情報共有

サイバー攻撃が発生した場合には、国の法令、制度等に基づき非営利でインシデント対応相談や分析、情報共有活動を行う専門機関やセキュリティベンダーといった専門組織に対して、マルウェア情報等攻撃者による攻撃活動やまたはその痕跡を示す攻撃技術情報を共有することで、攻撃原因や被害範囲の特定を進めることが望ましい。

また、原因の特定を行うにあたり、専門組織に対してセカンドオピニオン的な相談を行うことが望ましい。

ウ．国、港湾管理者等への情報共有

サイバー攻撃等の意図的な原因、機器等の故障等の偶発的な原因、自然災害等の環境的な原因によるシステム障害が発生し、業務への影響が生じた場合、管轄される地域の地方運輸局等の港運担当課へ情報共有を行う。

また、港湾内の状況把握の観点から、港湾管理者に対しても情報共有を行うとともに、港湾管理者は管轄される地域の地方整備局等の危機管理担当課へ情報共有を行う。

なお、サイバー攻撃が発生した場合には、所轄の都道府県警察に通報を行うこと。

エ．対外的な情報発信

システム障害等により業務への影響が生じた場合、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。

オ．窓口担当者の指定

上記の情報共有や情報発信を行う際は、情報提供及び問合せ対応の窓口を設定すること。なお、問合せが集中する恐れがあることから、複数名を指定しておくことが望ましい。また、港湾管理者と事前に役割分担をしておくことも有効である。

（3）BCP

事業の継続を目的として、優先する業務、必要な対策を決定するまでの過程、業務継続方法、連携を要する関連部門、対外的な情報発信等を規定する BCP を策定すること。なお、自然災害を想定した BCP は多くの TOS 運用者において策定されているものの、システム障害を想定した BCP を策定している事例はほとんど見られなかったことから、システム障害時に特に留意すべき点を以下に示す。

ア．システムの障害調査に係る対応手順

システム障害の原因を調査することは、障害からの復旧のほか、再発防止策の検討のためにも重要である。システム障害発生時の情報連絡先に加え、調査の方法（委託先等）についても事前に整理しておくこと。調査の委託先については、システム機器の障害の場合等は、TOS のシステム保守会社及びシステム開発会社が想定されるが、特に、サイバー攻撃等が疑われる場合は、セキュリティベンダー、セキュリ

ティ専門機関等のサイバーセキュリティ専門家の助言を求めることが望ましい。

なお、システム障害の調査のためには障害発生時の環境を保持しておく必要があることから、システムの復旧作業の開始とトレードオフの関係となりうることに留意する必要がある。

イ．システムの復旧に係る対応手順

システムの復旧に係る対応手順の策定の際には、システムの障害調査に係る対応手順を踏まえた上で検討すること。

システムの復旧に係る対応手順については、実際に復旧作業を行う TOS のシステム保守会社やシステム開発会社と事前に共有しておくこと。

また、サイバー攻撃を受けた後に運用を再開する際には、システムが十分な情報セキュリティ対策が取られている状態であるかどうかを確認することが望ましい。

ウ．システムを利用しない荷役等の手順

システム障害発生時の業務継続の手段として、TOS を利用せずにマニュアル作業によるコンテナの目視確認、データ照合等を行い、本船荷役を実施すること等が想定される。

システムを利用しない場合の荷役等の手順について、取扱貨物量等を踏まえ必要に応じて予め整理しておくこと。

（4）情報セキュリティに関する情報収集

セキュリティインシデントの情報更新速度は非常に速いため、日頃から情報収集を継続的に実施する必要がある。また、情報セキュリティ事案が発生した際の初動対応時の相談先となりうることから、セキュリティベンダー、セキュリティ専門機関、都道府県警察等と平時から情報交換等を行うことが望ましい。

また、TOS の情報セキュリティに関するグッドプラクティスやヒヤリハットを各 TOS の情報セキュリティ担当者間で共有する枠組みを構築することが望ましい。

（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・訓練

情報セキュリティ対策の実施に当たっては、システム業務に従事する人材のみならず、システムユーザや PC 操作者に対しても必要な措置（情報セキュリティポリシー等の規程に基づく操作等）を求める必要がある。情報セキュリティ関係規程を組織全体に周知する等、組織内における情報セキュリティ意識の向上を図るとともに、情報セキュリティに係る教育・訓練等も実施すること。

（6）TOS 利用契約時における責任分界、保険加入の検討

TOS の障害によりコンテナターミナルの機能が停止し、船舶運航会社、荷主等に追加費用や損害が発生した場合、損害賠償請求を受けることが想定される。

TOS の所有者と利用者である港湾運送事業者が異なる場合、両者の間での責任分界について予め整理しておくことが望ましい。また、サイバー攻撃等の外的要因によるシステム障害発生に備えて、サイバー保険に加入しておくことも有効である。

（7）脆弱性や設定不備の定期検査

サーバ装置、端末及びネットワーク機器上で利用しているソフトウェアについて、当該ソフトウェアに関する脆弱性対策に必要となる情報を収集し、脆弱性対策の状況を定期的に確認すること。脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及びネットワーク機器上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用、ソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、適切な措置を講ずること。

（8）情報セキュリティ対策の監査

情報セキュリティの確保のためには、情報セキュリティに関する組織内の基準の妥当性、対策の妥当性、体制等の実効性の有無を確認する必要がある。そのため、組織による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を定期的に実施すること。

5．情報セキュリティ対策等の推進のための制度的措置

（1）基本的考え方

港湾は、国、港湾管理者、港湾運送事業者等の関係者が、様々な情報システムを使用して役務の提供等を行うことで、国民生活及び経済活動の基盤として機能している営造物である。港湾で使用されるこれらのシステムについては、その機能が停止・低下するリスクを低減するため、各システムを使用する事業者や各システムの所有者等が、情報セキュリティ対策を適切に実施する必要がある。

特にコンテナターミナルについては、我が国の物流において大切な役割を果たしていること、またその機能が損なわれた場合には広範囲にわたる多様な荷主に影響を及ぼすおそれがあること等から、安定的に機能することが極めて重要である。

また、入出港や係留施設等を利用するための手続に使用される港湾管理者のシステムは、主に船舶単位で処理されるものであり件数が少なく、BCP 等の措置を適切に講じることでマニュアルでの手続で代替し得るのに対し、コンテナターミナルの TOS はコンテナ単位の膨大な情報を処理するため、システムが停止した場合等においてマニュアルで代替することが困難なターミナルが生じると考えられ、その情報セキュリティ対策は極めて重要である。

国は、出入管理情報システム等自らのシステムの情報セキュリティ対策を適切に

実施するとともに、コンテナターミナルの TOS をはじめとする港湾で使用されるシステムの情報セキュリティ対策が効果的に実施されるよう、国、港湾管理者、港湾運送事業者等の多様な関係者の連携等を促進することが適当である。

（2）港湾運送事業法に基づく措置について

５.（1）でも示されているとおり、コンテナターミナルが安定的に機能することは極めて重要である。コンテナターミナルの TOS が停止した場合、TOS を介さずに荷役を継続することが困難なターミナルも生じ得ると考えられ、その情報セキュリティ対策は極めて重要である。

このような状況を踏まえるならば、港湾運送の安定的な提供を図る観点から、TOS の情報セキュリティ対策の状況を的確に把握するとともに、TOS の情報セキュリティ対策の強化・底上げを図ることが必要である。このためにはコンテナターミナルにおいて一般港湾運送事業者が使用する 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を図ることが求められる。

具体的には、一般港湾運送事業の許可を受けようとする者がコンテナターミナルで TOS を使用しようとする場合に、港湾運送事業への参入等に際して審査を受ける必要がある事業計画に TOS の概要や情報セキュリティの確保に関する事項を記載することが求められる。一般港湾運送事業者として事業計画に定める業務を確保することを通じ、情報セキュリティを担保するものである。

この制度設計に際して、事業計画に記載する TOS の概要については、外部との接続状況等を把握し、必要となるセキュリティ対策を見極めるために、ネットワーク構成がわかるシステム概要図の提出を求めるとともに、システム面や体制面について特に重要な情報セキュリティ対策の実施を求める必要がある。また、名古屋港の情報セキュリティ事案がそうであったように TOS の使用者（一般港湾運送事業者）と所有者が異なる場合に情報セキュリティ対策の確保の実効性を担保するために、TOS の使用者と所有者との間において、一般港湾運送事業の適正かつ確実な遂行の確保に必要な措置を講ずるための TOS の運用及び管理に関する契約を締結していることを証する書類の提出が求められる。さらに、コンテナターミナルの重要性やシステム依存度を考慮し、特にコンテナ取扱貨物量の多い港湾については、そのほかの港湾で求めるセキュリティレベルより高いレベルの対策を求める必要がある。

なお、港湾運送事業者が実施する情報セキュリティ対策に対する国の関与については、港湾運送事業者に過度な負担とならないよう、港湾運送事業の継続のため真に必要なものに限定することにも配慮する必要がある。

（3）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について

「３．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」及び「４．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」において、TOSを運用する上で必要な情報セキュリティ対策について掲げたところであるが、これは法令や制度に基づいたものではなく任意の対策となる。港湾分野におけるデジタル化が進展する中で、多様な関係者が様々な形態でシステムを導入・運用していることを踏まえると、港湾分野においても面的に情報セキュリティ対策を着実に実施する必要がある。

他の分野においては、サイバーセキュリティ基本法に基づき、重要インフラ事業者[8]は、重要インフラ防護に係る基本的な枠組みを定めた官民共通の「重要インフラのサイバーセキュリティに係る行動計画」（以下「行動計画」という。）に基づいて対策を講じている。具体的な重要インフラ事業者は、14 の重要インフラ分野[9]に属する事業を行う者のうち、行動計画において指定された事業者とされており、重要インフラ事業者は、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めることとされている。

行動計画における主な取組としては、

①重要インフラ事業者等は組織全体としてサイバーセキュリティを確保するとともに、官民の相互連携を密にすること等による障害対応体制を強化

②重要インフラ事業者等の関係主体における「安全基準等」の整備及び浸透の取組を推進する等による安全基準等の整備及び浸透

③個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、官民間や分野内外間における情報共有体制の更なる強化による情報共有体制の強化

④自組織に適した防護対策の計画・実施、評価・改善の繰り返しによる継続的な取組を推進する等によるリスクマネジメントの活用

⑤障害対応体制の有効性検証、人材育成、関係機関との連携、国際連携、広報広聴活動等、行動計画の全体を支える共通基盤的な取組による防護基盤の強化

が掲げられており、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していくこととされている。

---

8 重要インフラ事業者とは、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者。

9「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の 14 分野（令和 5 年 11 月現在）

本検討委員会における

・最新情報やトレンドを反映した対策の実施

・適切なバックアップ等による事業継続

・多様な関係者などの港湾の特性を踏まえた体制の構築

といった議論を踏まえ、これらの対策を制度的にどう担保していくか検討する必要がある。重要インフラ分野に「港湾」が新たに位置づけられることになれば、上記で述べた①障害対応体制の強化、②安全基準等の整備及び浸透、③情報共有体制の強化、④リスクマネジメントの活用、⑤防護基盤の強化に取り組みながら、重要インフラ事業者は自主的かつ積極的にサイバーセキュリティの確保に努めつつ、かつ、情報共有体制を構築することで縦横の連携を深めていくこととなる。

港湾分野においても面的に情報セキュリティを高めていくためには、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であることから、重要インフラ分野に「港湾分野」を位置づける方向で検討を進めていくことが求められる。

（4）経済安全保障の観点からの措置について

「3．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」において、TOS の開発・保守等について外部委託を行う場合の情報セキュリティの確保を掲げたところであるが、我が国の産業や国民生活を支える重要なインフラである港湾においては、経済安全保障の観点からの措置も重要である。

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（以下「経済安全保障推進法」という。）においては、14 の分野[10]で、国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの[11]の提供を行う事業を定め、当該事業を行う者のうち一定の基準に該当するものとして指定された者が対象の設備の導入又は維持管理等の委託を行うときに、主務大臣が事前審査を行うこととされている。

---

10 「電気」、「ガス」、「石油」、「水道」、「鉄道」、「貨物自動車運送」、「外航貨物」、「航空」、「空港」、「電気通信」、「放送」、「郵便」、「金融」及び「クレジットカード」の 14 分野。

11 「国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの」とは、特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（令和 5 年 4 月 28 日閣議決定。以下「基本指針」という。）において、①国民生活又は経済活動が依存している役務であって、その利用を欠くことにより、広範囲又は大規模な社会的混乱を生ずるなどの経済・社会秩序の平穏を損なう事態が生じ得るもの、②国民の生存に不可欠な役務であって、その代替が困難であるものと例示されている。

インフラ事業者が利用するICT機器の高度化やそのサプライチェーンの複雑化・グローバル化を背景に、サプライチェーンの過程で不正機能が埋め込まれる可能性や、機器の脆弱性に関する情報がインフラ事業者の意図に反して共有される可能性等が高まっている。このため、インフラ事業者が利用するICT機器が、役務の安定的な提供を妨害する行為の手段として我が国の外部から使用されるおそれが増大しており、こうしたことを背景として経済安全保障推進法に事前審査制度が設けられた。コンテナターミナルのTOSも、そのように使用されるおそれがないと言うことはできないが、港湾運送事業は当該事前審査制度の対象とはされていない。

上述の「（1）基本的考え方」のとおり、港湾における各種のシステムのうち、入出港や係留施設等を利用するための手続に使用される港湾管理者のシステムは、主に船舶単位で処理されるものであり件数が少なく、BCP等の措置を適切に講じることでマニュアルでの手続で代替し得るのに対し、港湾運送事業者のうち一般港湾運送事業者が使用するコンテナターミナルのTOSはコンテナ単位の膨大な情報を処理するため、システムが停止した場合等においてマニュアルで代替することが困難である。また、上述のとおりコンテナターミナルは我が国の物流において重要な役割を果たしていることから、規模が特に大きい港湾において一般港湾運送事業者が使用するTOSについては、その機能が停止・低下し、荷役作業に支障が生じた場合、影響が甚大となるおそれがある。

以上を踏まえれば、港湾における対策については、上述の「（2）港湾運送事業法に基づく措置について」によりTOSの情報セキュリティ対策の確保状況を国が審査する仕組みを導入した上で、さらに経済安全保障の観点からも国として積極的な関与を行うため、経済安全保障推進法の趣旨も踏まえ、コンテナターミナルにおいてTOSを使用して役務の提供を行う一般港湾運送事業を経済安全保障推進法の対象事業とすることが必要であると考えられる。

一方、経済安全保障推進法の運用においては、特定社会基盤事業者や特定重要設備等の対象範囲について、安全保障の確保のために真に必要な範囲に限定する必要があるとされている[12]。このため、一般港湾運送事業を経済安全保障推進法の対象事業とする場合、制度の対象とする事業者及び設備の範囲については、このような経済安全保障推進法の趣旨も十分に踏まえつつ検討する必要がある。

また、上述の「（3）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について」により事業者による主体的な対策を促進することも必要と考えられる。

6．今後の対応について

以上、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的に実施す

[12] 基本指針参照。

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示した。今後、これら対応策を実効あるものとするために、国は、緊急的に実施すべき対応策の周知、説明会の開催等を通じ港湾関係者の理解の増進に努める必要がある。また、港湾の情報セキュリティ対策をより確実に実施するため、国は、諸外国の港湾におけるサイバー攻撃事例の調査、ガイドラインの策定、研修の実施などを通じ、港湾関係者への有益な情報の提供に努めるとともに、事案の発生に備え広域的な連携を促進することが求められる。

これらを通じ、情報セキュリティ対策の必要性と重要性が港湾関係者に認識され、我が国の港湾における情報セキュリティ対策の向上が図られるものと確信している。

本委員会としては、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、コンテナターミナルにおける情報セキュリティ対策等について、必要に応じ改めて検討することとする。