中間取りまとめ①に掲げた対策等の現行制度における位置づけ

国土交通省

資料２－５

中間とりまとめ①に掲げた対策等の推進に向け、港湾の特性を的確に捉えたサイバーセキュリティ対策を行うための対応や、システムの導入等を委託する場合における安全性確保のあり方に関連する現行制度（サイバーセキュリティ政策及び経済安全保障政策等）との関係を整理した。

＜現行制度におけるサイバーセキュリティ対策に係るガイドライン＞

・サイバーセキュリティ基本法に基づく「重要インフラの情報セキュリティ対策に係る第４次行動計画」及び「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」に則り、**「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」**（以下「安全ガイドライン」という。）が策定されている。

・「安全ガイドライン」には、情報セキュリティ対策を実施する場合に何らかの対処がなされていることが望ましい項目及び対処すべき内容が列挙されている。

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

中間とりまとめ①に掲げた対策等

（）の番号は中間とりまとめ①の３．の番号に対応

（１）資産の把握

・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）の接続状況等の把握

現行制度における位置づけ

○情報システムの構成要素の運用に関する対策※

・主管する範囲の端末で利用されているすべてのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

・サーバ装置について、構成管理・変更管理を実施すること。

・通信回線及び回線装置について、構成管理・変更管理を実施すること。

（参考）

【第１回検討会より】

・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。

※安全ガイドラインより抜粋

中間取りまとめ①に掲げた対策等の現行制度における位置づけ

国土交通省

中間とりまとめ①に掲げた対策等	現行制度における位置づけ	（参考）
（3）サーバ機器、システム内のネットワーク機器 ・セキュリティ対策ソフトの導入 ・ソフトウェアの情報を定期的に確認し更新 ・管理者ID/パスワードの厳格化、多要素認証の導入	**○サーバ機器、システム内のネットワーク機器に関する対策※** ・脆弱性対策の状況の定期的な確認により、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、端末及び通信回線装置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又は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、措置を講ずること。 ・顧客向けに提供するインターネットサービスには、多要素認証機能の実装等の対策を講ずること。	
外部との接続 **（2）外部との接続** 【VPN】 ・接続元IPアドレスの指定 ・多要素認証の導入 ・アカウントロック機能の実装 ・不正ログイン試行を検知する機能 【外部記録媒体（USBメモリ等）】 ・ウイルスチェック 【専用線、NAT】 ・ファイアウォールの設置	**○外部との接続に関する対策※** ・VPN 環境を整備してリモートアクセス環境を構築する場合には、通信を行う端末の識別又は認証やリモートアクセス環境を利用する者の認証等を含む対策を講ずることが望ましい。 ・IoT 機器を含む特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う等の対策を講ずること。 ・外部電磁的記録媒体による情報のやりとりにおける安全確保のために、情報の取り扱いに関する利用手順を定めるなど必要な措置を講ずること。 **【追加検討が必要な事項】** ・不正ログイン試行の検知やウィルスチェックなど具体的な対策を明記した追記の検討が必要。	【名古屋港事案】 ・VPN機器がウイルスの侵入経路の可能性が高い。 【第１回検討会より】 ・保守に利用する外部接続部分のセキュリティ対策は見落としがち。

※安全ガイドラインより抜粋

中間取りまとめ①に掲げた対策等の現行制度における位置づけ

国土交通省

外部との接続

中間とりまとめ①に掲げた対策等

（5）クラウド利用時の対策

・アクセス制限（IPアドレス等）
・アクセスログ等の証跡の保存及び提供
・脆弱性対策の実施内容の確認　等

（6）TOSと連携している外部機器への影響

・現状の再認識
（接続機器、外部との接続）
・必要な対策

（4）バックアップ

・バックアップを取るべき対象
（システム、データ、ログ等）
・取得頻度
・バックアップの複数保存
・バックアップの保存場所

現行制度における位置づけ

○クラウドサービスの利用に関する対策※

・クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める。
・クラウドサービスを利用する際には、以下をセキュリティ要件に含めることが望ましい。
　・アクセス制限（IP アドレス等）
　・アクセスログ等の証跡の保存及び提供
　・脆弱性対策の実施内容の確認　　等

○組織・体制の確立に関する対策※

・重要インフラ事業者等の保有する重要なシステム等に係る情報セキュリティの確保については、各重要インフラ事業者等が自らの管理下にある情報資産に責任を持ち、それぞれの事業形態や情報システムの形態に適応した情報セキュリティ対策を講じていくことが原則。

【追加検討が必要な事項】

・TOSに特化した対策の必要性について検討が必要。

○情報システムのバックアップに関する対策※

・必要な情報のバックアップを取得し、同じ重要インフラサービス障害で同時に被災しない場所に保存することはもとより、特に重要な業務を支える情報システムについては、バックアップシステムを整備すること。
・情報システムのバックアップに関し、BCP 等を検討する際には、以下の点を考慮することが望ましい。
　・バックアップの対象
　・バックアップの周期、世代管理の方法
　・バックアップを保存する電磁的記録媒体等の種類　　等

（参考）

【名古屋港事案】
・原因を分析するためのログが暗号化被害のため取得できなかった。
・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。

【第１回検討会より】
・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。

※安全ガイドラインより抜粋

中間取りまとめ①に掲げた対策等の現行制度における位置づけ

国土交通省

中間とりまとめ①に掲げた対策等	現行制度における位置づけ
（7）（TOSの開発・保守等の）外部委託を行う場合の情報セキュリティの確保	**〇外部委託実施における情報セキュリティ確保策※** ・外部委託を実施する際に、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、重要インフラサービス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外部委託に伴う契約を取り交わすこと。 **〇システムの導入等に関する審査制度** ・TOS等のシステムの導入等を審査対象とする**港湾関係法令はない。** ・経済安全保障推進法では、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役務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者が重要な設備・プログラム等の導入及び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しているが、**港湾関係の事業はその対象となっていない。**

（参考）

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

中間とりまとめ①に掲げた対策等	現行制度における位置づけ
（）の番号は中間とりまとめ①の4．の番号に対応 （3）業務継続計画（BCP） ・システムの障害調査にかかる対応手順 ・システムの復旧にかかる対応手順 ・システムを利用しない荷役等の手順	**〇事業継続計画の整備に関する対策※** ・初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画（BCP）」を策定する。 ・BCP 等においては、重要インフラサービス障害発生時における優先業務、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等を規定する。

（参考）

【第1回検討会より】
・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。

※安全ガイドラインより抜粋

中間取りまとめ①に掲げた対策等の現行制度における位置づけ

国土交通省

体制の構築

中間とりまとめ①に掲げた対策等	現行制度における位置づけ	（参考）
（1）組織・体制の確立 ・セキュリティ担当者等の指定	○組織・体制の確立に関する対策※ ・重要インフラ事業者等は、組織の幹部の関与を明確にするとともにその責任の所在を明確にするため、情報セキュリティを統括する長として最高情報セキュリティ責任者等、情報セキュリティ対策を進める単位ごとに情報セキュリティ責任者を定めること。	【第１回検討会より】 ・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。
（2）情報連絡体制 （クライシスマネジメント） ・自組織内の情報共有 ・国、自治体等への情報共有 ・対外的な情報発信 ・窓口担当者の指定	○関係機関との情報共有に関する対策※ ・情報セキュリティインシデントが発生した際、直ちに最高情報セキュリティ責任者への報告が行われる体制を整備すること。 ・国民生活及び社会経済活動に影響を与える重要インフラサービス障害が発生した場合、国土交通省へ情報連絡を行うこと。 【追加検討が必要な事項】 ・現状は、物流分野の重要インフラ事業者である大手港湾運送事業者等のみが関係機関との情報共有体制が整っているので、その他関係者を含む情報共有体制の構築について検討が必要。 ・その他関係者においても初動対応時にセキュリティの専門家の意見を聞くことができる体制構築の検討が必要。	【名古屋港事案】 ・初動対応時にセキュリティの専門家の意見を聞く場面がなかった。 【第１回検討会より】 ・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。

※安全ガイドラインより抜粋

中間取りまとめ①に掲げた対策等の現行制度における位置づけ

国土交通省

体制の構築

中間とりまとめ①に掲げた対策等	現行制度における位置づけ	（参考）
（4）情報セキュリティに関する情報収集（リスクマネジメント） ・日頃からの情報収集 ・セキュリティベンダー、セキュリティ専門機関や都道府県警察等との平時からの情報交換 ・ベストプラクティスやヒヤリハットの共有	**○関係機関との情報共有に関する対策※** ・重要インフラ事業者等は、所属するセプターにおいて、相互に重要インフラサービス障害やサイバー攻撃に係る情報、復旧手法情報、早期警戒情報等の共有を行うこと。 **【追加検討が必要な事項】** ・物流分野の重要インフラ事業者である大手港湾運送事業者等以外の関係者においても最新の脅威や脆弱性情報を入手する方法の検討が必要。	【第１回検討会より】 ・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。 ・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。 ・感度良く業界全体 で情報を把握しておくべき。
（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 ・情報セキュリティ関係規定を組織全体に周知 ・情報セキュリティに係る教育・研修の実施	**○人材育成・配置・ノウハウの蓄積に関する対策※** ・情報セキュリティ関係規程について、取扱者を適切に教育・配置するための計画を立案するとともに、その実施体制及び教育のための資料を整備し、ノウハウの蓄積に努めること。 ・教育内容としては、以下のような項目を含むことが望ましい。 ・ 情報の取扱い（格付け及び取扱制限） ・ 情報セキュリティポリシー ・ 情報セキュリティへの脅威と対策 ・ 重要インフラサービス障害発生時の対処手順及び体制	

※安全ガイドラインより抜粋

中間取りまとめ①に掲げた対策等の現行制度における位置づけ

国土交通省

中間とりまとめ①に掲げた対策等	現行制度における位置づけ	（参考）
（6）契約時における責任分界保険加入の検討 ・責任分界の整理 ・サイバー保険への加入の検討	**○外部委託実施における情報セキュリティ確保策※** ・システム管理者は、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書を提出させること。 **【追加検討が必要な事項】** ・「サイバー保険への加入」等の具体的対策を促す例示の追記の検討が必要。	【第１回検討会より】 ・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。
（7）脆弱性や設定不備の定期検査 ・ソフトウェアに関する脆弱性対策に必要な情報の収集 ・脆弱性対策の定期的な確認 ・脆弱性対策の実施	**○ソフトウェアに関する脆弱性対策に関する対策※** ・サーバ装置、端末及び通信回線装置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。 ・システム管理者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合、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又は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、措置を講ずること。	
（8）情報セキュリティ対策の監査 ・自己点検および第三者の情報セキュリティ監査を定期的に実施	**○情報セキュリティ対策の監査に関する対策※** ・取扱者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実施することが必要。 **【追加検討が必要な事項】** ・実施すべき監査のチェックリスト等の具体的対策を促す例示の追記の検討が必要。	

定期検査・監査

※安全ガイドラインより抜粋