「港湾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2版）」

に関するＱ＆Ａ

令和７年５月　日

国土交通省港湾局

目次

1　ガイドラインの位置付けについて

Q1. 重要インフラ事業者とは何か？

A. サイバーセキュリティ基本法第 12 条 2 項第 3 号に規定する重要社会基盤事業者（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じるものに関する事業を行う者）であり、港湾の場合、主要な港湾運送事業者や港湾管理者等である。

Q2. 本ガイドラインはTOSを所有する重要インフラ事業者を主にした内容となっているように思うが、それ以外の事業者はどのように活用すればいいのか？

A. 本ガイドラインでは、主にコンテナターミナルで使用されている TOS を中心とした記載になってはいるが、コンテナ貨物以外でもシステムによって荷役等を管理している場合も想定されるため、このようなシステムが急遽使用できなくなった場合に事業が停止するなどの影響が大きいと考えられる場合も含めて、その対応策の参考としていただきたいと考えている。

Q3. TOS 以外のシステムで、具体的に想定されているシステムはどのようなものか？

A. コンテナターミナル以外のターミナル（フェリー・ROROターミナル、バルクターミナル等）においても荷役のオペレーションシステムが導入されている場合が有ると推察される。また、コンテナターミナルにおいてもTOS以外のシステムが停止すると、荷役が停止する事態が発生するようなシステムが有ると推察される。どのシステムが保護対象となるかについては、それぞれの重要インフラ事業者等の責任において、システム停止によるサービス障害が、社会経済活動等に多大な影響を与えるシステムを検討・抽出していただきたい。

Q4. 本ガイドラインの法的位置付けは？

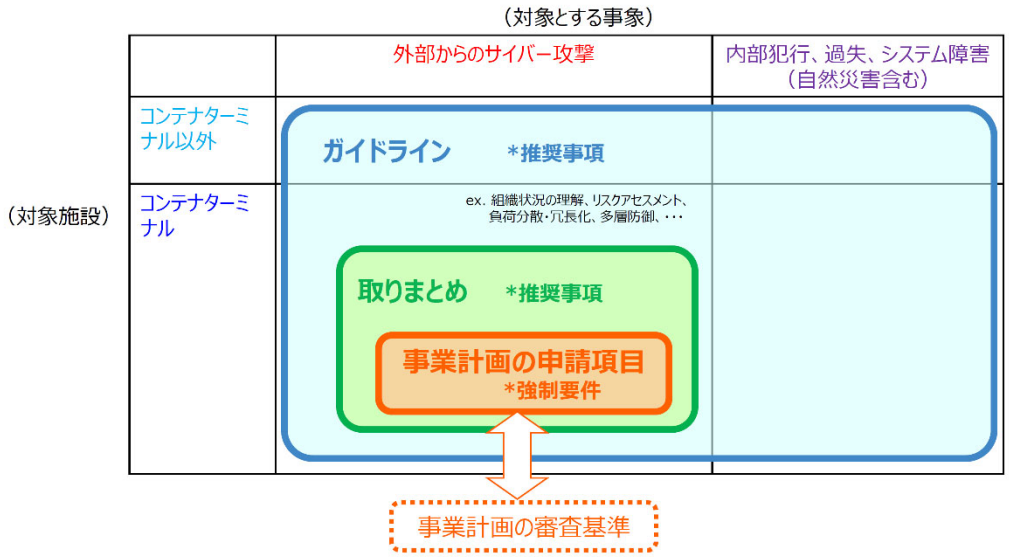
A. 本ガイドラインは、サイバーセキュリティ基本法に基づき、所管省庁である国土交通省港湾局が定めるガイドラインとして、推奨事項を列挙しているものである。

Q5. ガイドラインで求める対策と港湾運送事業法の事業計画の申請項目との関係は？

A. 港湾運送事業法では、改正港湾運送事業法施行規則を施行（令和 6 年 3 月 31 日）し、港湾運送事業者に対し、一般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の記載を求めている。これにより、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ている。

港湾運送事業法の事業計画で求める内容が強制要件であるのに対し、本ガイドラインで求める対策は重要インフラサービスの継続性維持に向けて、重要インフラ事業者等がサイバーセキュリティ確保に向けて、自主的に取組、対策の実施や検証にあたっての目標を定めることを目的として策定したものであり、国が定めるガイドラインとして推奨事項を列挙したものである。

なお、本ガイドラインで記載している対策の例示(〔具体例〕)のうち、港湾運送事業法における事業計画の届け出で必要となる項目(強制要件)については、網掛け(全ての港が対象)、下線(特定の港が対象)を付している。



※「取りまとめ」は、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(令和6年1月)

図 ガイドラインと「取りまとめ」及び港湾運送事業法の事業計画申請項目との関係

Q6. 本ガイドラインの実施状況について国による監査はあるのか？

A. 本ガイドラインは、重要インフラ事業者等がサイバーセキュリティ確保に向けて、自主的に取組、対策の実施や検証にあたっての目標を定めることを目的として策定したものであり、国が定めるガイドラインとして推奨事項を列挙したものであり、国土交通省港湾局による監査を行うものではない。
なお、本ガイドラインでは、ガイドラインの実施状況について、各重要インフラ事業者等において定期的な監査(自己点検及び独立性を有する者による外部監査)を実施することを求めている。
また、港湾運送事業法では、特定の港については、定期的な監査(自己点検及び独立性を有する者による外部監査)を強制要件としている。

Q7. 本ガイドラインの対策を実施していない場合、罰則規定はあるのか？

A. 本ガイドラインは、重要インフラ事業者等がサイバーセキュリティ確保に向けて、自主的に取組、対策の実施や検証にあたっての目標を定めることを目的として策定したものであり、国が定めるガイドラインとして推奨事項を列挙したものであり、本ガイドラインの対策を実施していない場合であっても、重要インフラ事業者等に罰則を求めるものではない
なお、法令による罰則規定は無いが、本ガイドラインに記載する対策等、情報セキュリティ確保に関して適切な対策がとられていない状況下でサイバー攻撃を受け、重要サービスが停止し、自組織や第三者に損害が生じた場合には、損害賠償責任を問われ得る点に留意が必要である。

2　セキュリティ対策の実施方法等について

Q8. 最高情報セキュリティ責任者には、どのような資質・資格要件が求められるか？

A. 最高情報セキュリティ責任者（CISO）は、サイバーセキュリティに関する知見を有する者であるとともに、組織内の職階において、平時に、またとりわけ有事に、組織トップと直接コミュニケーションできる者として位置付けられるべきであり、経営者層に相当する者の中から任命されることが望ましい（役員クラスが相当）。

（参考：「医療情報システムの安全管理に関するガイドライン第 6.0 版」に関するQ&A」（令和 5 年 9 月、厚生労働省））

Q9. CSIRTとして想定される担当部門・担当者は？

A. セキュリティインシデントが発生した際に対応するチームとなる CSIRT の設置にあたっては、一般社団法人 JPCERT コーディネーションセンターの「CSIRT マテリアル」や、一般社団法人日本シーサート協議会の「CSIRT 人材の定義と確保」などが参考となる。

港湾分野で想定されるインシデント対応体制の例は、「セキュリティ責任者編 1.9.1CSIRT 等の整備、関連部門との役割分担」を参照のこと。

Q10. リスクアセスメントをどのように実施すれば良いか？

A. リスクアセスメントのプロセスとしては、①リスクアセスメントの対象の特定、②リスク特定、③リスク分析、④リスク評価となる。

リスクアセスメントの具体的な進め方については、NISC「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」（令和 5 年 7 月）が参考となる。

Q11. マルウェア対策としてどのような対策が有効か？

A. マルウェアからの保護の方法としては、現時点では以下の対応が有効と考えられる。

①マクロ等の埋め込みコードの実行を全ての機器において既定で無効とする。業務においてコードを実行する必要がある場合、許可されたユーザーが特定の状況下で実行できることを承認する仕組みを構築する。

②マルウェアの検知率向上が期待されるマルチエンジン型のマルウェア検知ソフトの利用やシステム負荷を抑えつつ未知の脅威に対応できることを特徴とするマルウェア対策 機能 等の導入を検討する。

③被害が発生した際の、攻撃の拡散に備えた対策例として、ネットワークセグメント分割（重要インフラの分離）、 IPSIPS9 プロキシサーバ（不審な外部通信の遮断）、 EDREDR10（影響範囲の特定と被害端末の隔離 、 NDR（ネットワーク全体の包括的な監視と脅威検知等がある。

（参考：「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」（令和 5 年 7 月、NISC））

Q12. 不正アクセスへの対策を講じる際、どのような留意事項があるか？

A. クラッカーや不正ソフトウェアによる攻撃から情報を保護するための一つの手段として、ファイアウォールの導入があるが、これに加えて、不正な攻撃を検知するシステムファイアウォールは、「パケットフィルタリング」、「アプリケーションゲートウェイ」、「ステートフルインスペクション」等の各種方式がある。また、その設定によっても動作機能が異なるので、単にファイアウォールを導入すれば安心というものではない。単純な「パケットフィルタリング」で十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望まれる。

部外者により物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、不正ソフトウェアが混入したり、 サーバやネットワーク機器に対して攻撃（サービス不能攻撃 DoS Denial of Service 等）を行ったりすることや、不正にネットワーク上のデータを傍受したり改ざんしたりすることが可能となる。

不正なコンピュータの物理的な接続に対する対策を行う場合、一般的に MAC アドレスを用いてコンピュータを識別する場合が多いが、 MAC アドレスは改ざん可能なため、そのことを念頭に置いた上で対策を行う必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に実施するかが重要であり、特に、“なりすまし”の防止は確実に行う必要がある。

無線 LAN のアクセスポイントを複数設置して運用する場合等、マネジメントの複雑さが増し、侵入の危険が高まるような設置をする場合には、一層留意が必要である。

また、ネットワーク上を流れる情報の盗聴を防止するために、暗号化等による“情報漏えい”への対策も必要となる。

（参考：「医療情報システムの安全管理に関するガイドライン第 6.0 版」に関するQ&A」（令和 5 年 9 月、厚生労働省））

Q13. バックアップの取得にあたって、どのような留意事項があるか？

A. バックアップの取得範囲として、 通常、フルバックアップ、差分バックアップ、増分バックアップなどがあり、適切に組み合わせて、対応することになる。そのうえでさらに具体的な例として、日次で差分バックアップ、週次でフルバックアップを行う場合、前々週以前のフルバックアップ及びその週以前の日時の差分バックアップは、ネットワークから切り離した記録媒体で保管すること（磁気テープ、DVD、 Blu-Ray 等）あるいは論理的に書き込み禁止（磁気ディスク等）の状態にする等の対策が必要となる。

最近ではクラウドサービスを利用したバックアップを行うことも考えられる。例えば、原本データ以外にクラウド上でバックアップを取得する場合、バックアップデータを追記できない設定としたり、複数のバックアップデータを取得したりするなどの方式で、複数方式によるバックアップを行うことが想定される。

（参考：「医療情報システムの安全管理に関するガイドライン第 6.0 版」に関するQ&A」（令和 5 年 9 月、厚生労働省））

Q14. ログの取得にあたって、どのような留意事項があるか？

A. システム及びネットワーク機器等のアクセス・認証ログや通信ログ、セキュリティ対策システムのイベントなどセキュリティの確保に必要なログを、検知及びインシデント対応で使用するために収集し、保存する。

定期的又は適宜、保存したログの点検及び分析を行う。

ログを改ざん、削除から保護するための対策を行う。また、イベントログなど重要なログソースが無効化された場合、セキュリティ担当者に通知する。ログ機能が非搭載の制御システムについては、 制御システムとの間の通信ログを収集する。

収集したログはツールや中央システム（SIEM 等）に一元的に保存され、許可された管理者のみがアクセスできるようにする。 ログの保存期間については、関連するガイドラインや、想定するリスクに基づき設定する。

（参考：「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」（令和 5 年 7 月、NISC））

Q15. コンティンジェンシープランと事業継続計画との関係は？

A. 「コンティンジェンシープラン」とは、重要インフラサービス障害の発生又はそのおそれがあることを認識した際に、経営層や職員等がまず実施すべき対応として、初動対応（緊急時対応）の方針、手順、態勢等を定めたもの。

「事業継続計画」とは、重要インフラサービス障害発生時において、サービスを許容可能な時間内に許容可能な水準まで復旧させることを目的とし、復旧に向けた目標水準、優先順位、その他の方針、手順、態勢等を定めたもの。

なお、コンティンジェンシープラン、事業継続計画の名称や記載の範囲、発動のタイミング等は分野や事業者等によって異なる場合があるため、サイバー攻撃リスクの特性等を考慮して策定・改定すべき対象ドキュメント適用対象）は各事業者等の状況に応じて検討される必要がある。

サイバー攻撃リスクの特性については、NISC「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」（令和 5 年 7 月）が参考となる。

Q16. 復旧目標はどのような考えで設定すれば良いか？

A. 復旧目標の設定にあたっては、当該港・ターミナルにおいて、どの程度の期間サービスを停止したら顧客を失うか等を勘案することが重要である。仮にサイバー攻撃により TOS が停止した場合には、緊急的にマニュアル作業で荷役を行うことも考えられるが、特に大規模な港湾の場合には、その対応は極めて限定的で、TOS が復旧しない限りは本格的な荷役再開は困難とみられる。一方で、TOS の復旧に要する期間は、その被害の範囲・程度によることになるため、一概に復旧目標時間を設定することは難しい面がある。しかしながら、TOS のネットワーク構成やバックアップ等の対策を検討する際の目標として、また、顧客への対外的な情報発信の意味でも、復旧目標（復旧日数や復旧レベル）を設定することが望ましい

Q17. インシデント対応手順での留意事項

A. 重要インフラサービス障害が発生した場合には、早急にその状況を把握し、被害の拡大防止、早期復旧のための対策を講ずる必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定められた責任者へ報告し、障害による影響や範囲をエスカレーションし、二次被害を最小限に抑えることが重要である。

インシデント発生時の対応としては、IPA「中小企業のためのセキュリティインシデント対応の手引き」、JPCERT コーディネーションセンター「インシデントハンドリングマニュアル」等が参考となる。

Q18. サイバー攻撃を受けた際にどこの専門機関に相談すれば良いか？

A. インシデント対応の観点として、「専門機関の相談窓口等への相談により、おおむね解決できる」ケースと、「セキュリティベンダ等に調査を依頼・契約しなければ解決できないケース」にわかれる。専門機関の窓口に相談した場合、情報共有の必要性があるかどうかも含めて、情報共有に関する相談が可能である。後者のケースであっても、専門企業から専門機関への相談・情報共有活動から追加の情報の入手をアドバイスされる場合がある。あるいは被害組織の判断として、セカンドオピニオン的に専門機関への相談を並行して行う場合もある。

どの専門窓口に相談あるいは共有を行えば良いかについては、基本的な考え方としては、距離が近い組織を選ぶという観点になる。例えば、サイバーセキュリティ協議会の構成員であれば、協議会の相談窓口が想定される。

各専門企業や専門機関では、それぞれ得意な分野や、行うことができる業務に違いがある。例えば、不正サイトのテイクダウン（無害化）などで海外の事業者に対する依頼・調整が必要となった場合、基本的には JPCERT/CC へ依頼がなされる。あるいは、特定の攻撃手法について集中的に追跡や対応を行っているかどうかも差異がある。

まずは、自組織が受けたと思われる攻撃手法に関する注意喚起やレポート／ブログ記事を掲載している専門機関に相談することが望ましい。あるいは、普段から業界団体、地域のコミュニティ活動、都道府県警察などからの案内などに専門機関による特設サイト、レポートの紹介や、相談窓口の案内が掲載されている場合があるので、そうした「目にしたことがある」相談先にコンタクトすることもわかりやすい方法である。

（参考：「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和 5 年 3 月、サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会））

Q19. 効果的な演習・訓練の実施方法・内容は？

A. リスクマネジメントによる事前対応と、障害発生時の危機管理の両面から、体制や取組の有効性を検証するため、 定期的に演習・訓練を実施する。重要インフラ全体の防護能力の観点からは、同業の重要インフラ事業者等やサプライチェーン、関係主体等との合同での演習・訓練やケーススタディ（他事業者の過去のインシデント対応事例の研究）の実施も期待される。なお、合同での演習・訓練には、内

閣サイバーセキュリティセンターが主催する「分野横断的演習」や、重要インフラ所管省庁やサイバーセキュリティ関係機関等の関係主体が主催するものがある。

（参考：「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」（令和５年７月、NISC））