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）

チェックリスト

令和７年５月

国土交通省港湾局

1. チェックリストの使い方

国土交通省

(1)はじめに

- 本チェックリストは、港湾分野における重要インフラ事業者等を対象とし、「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)」で記載した**取組の進捗状況を事業者等が自ら確認**できるよう作成したものです。

(2)チェックリストの目的

- 本チェックリストは、主に以下の目的で活用できます。
  - ✓ セキュリティ対策の現状の確認（対策実施の有無）ができる。
  - ✓ 現状で実施していない対策について、実施に向けた検討・準備状況や、実施に向けた課題等を記入することで、対策への取組方針を明確化できる。
  - ✓ 現状で実施できていない対策について、一定期間後（１年後）に、その進捗状況を確認できる。
  - ✓ 定期的なセキュリティ対策の見直しに役立てる。

(3)チェックリストの構成

- 本チェックリストは、「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)」に従い、読み手別に以下のチェックリストを用意しています。
  - ✓ 「経営者層編」
  - ✓ 「セキュリティ責任者編」
  - ✓ 「システム構築・運用者編」
  - ✓ 「港湾管理者等編」

1. チェックリストの使い方

(4)チェックリストの使い方

- 本チェックリストは、「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)」で記載した対策について、**ガイドラインの目次の順番に、対策の進捗状況を確認**できるようにしています。
- 対策実施の**現状の評価**と、**１年後の評価**を行うとともに、**備考欄に、対策実施に向けた検討・準備状況や、実施に向けた課題等を記入**することができるようにしています。
- 対策は、その内容により、**①組織的対策、②人的対策、③技術的対策、④物理的対策の４つで分類**し、対策実施にかかる労力・費用等をイメージできるようにしています。
  - ✓ 組織的対策・・・組織全体のセキュリティ体制を強化する対策（セキュリティ方針、体制構築、リスクマネジメント、関連文書規程作成、監査　等）
  - ✓ 人的対策　・・・従業員や利用者の意識を高める対策（従業員への教育・訓練、日々のセキュリティ運用　等）
  - ✓ 技術的対策・・・技術的な手段でセキュリティを強化する対策（ウイルス対策ソフト・ファイアウォール導入、アクセス制限、バックアップ　等）
  - ✓ 物理的対策・・・物理的な手段でセキュリティを強化する対策（サーバ等保管場所への侵入対策・出入管理、サーバ等の物理的保護　等）

(5)チェックリスト活用上の注意点

- 「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)」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、国が定める「ガイドライン」として推奨事項を列挙しているものであり、本チェックリストも、推奨事項としての対策に関する内容となっています。
- 本チェックリストの対策を全て行ったとしても対策とは完全とは限りません。
- 各事業者等の実情に応じた適切なセキュリティ対策を講じ、継続的な改善を図ってください。