苫小牧港管理組合情報セキュリティ基本方針

１　目的

本方針は、当管理組合が保有する情報資産の機密性、完全性及び可用性を確保・維持することを目的として、当管理組合が講ずる情報セキュリティ対策に関する基本的事項を定めるものである。

２　定義

(１)ネットワーク

コンピューター等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(２)情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(３)情報システム

コンピューター、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(４)情報セキュリティポリシー

本基本方針及び「苫小牧港管理組合情報セキュリティ対策基準に関する要綱」をいう。

(５)機密性

情報にアクセスが認められた者のみが、当該情報にアクセス可能な状態を保持することをいう。

(６)完全性

情報が破壊、改ざん又は消去されていない状態を保持することをいう。

(７)可用性

情報へのアクセスが認められた者が、必要なときに中断されることなく、当該情報にアクセスできる状態を確保することをいう。

(８)ネットワーク

コンピューター等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

(９)LGWAN 接続系

LGWAN に接続された情報システム及び当該情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

(10)インターネット接続系

インターネットメール、ホームページ管理システム等に係るインターネット接続された情報システム及び当該情報システムで取り扱うデータをいう。

(11)通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離し、安全性が確保された通信のみを許可することをいう。

(12)無害化通信

インターネットメール本文のテキスト化や端末への画面転送等を通じて、コンピューターウイルス等の不正プログラムの付着を防止し、安全性が確保された通信をいう。

3　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を講じる。

（1）サーバー攻撃（不正アクセス、ウイルス感染、サービス妨害等）及び部外者の侵入等の意図的要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模かつ広範囲に及ぶ疾病の流行による要員不足に伴うシステム運用の機能不全等

（5）電力供給、通信、水道供給のインフラ障害による波及等

4　適用範囲

(1)適用対象機関

本基本方針の適用対象は、管理者、監査委員、議会等、当管理組合の全ての実施機関並びに情報セキュリティ責任者が認める組織とする。

(2)対象情報資産

本基本方針の対象とする情報資産は、次のとおりとする。

① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

5　職員の遵守義務

職員は、情報セキュリティの重要性について共通認識を持ち、業務遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

６　情報セキュリティ対策

上記３に掲げる脅威から情報資産を保護するために、以下の対策を講じる。

（１）組織体制

情報セキュリティ対策を推進するため、全庁的な組織体制を確立する。

（２）情報資産の分類と管理

情報資産を機密性、完全性及び可用性に応じて分類し、分類に基づいた対策を実施する。

（３）情報システム全体の強靭性の向上

業務の効率性及び利便性を踏まえ、以下の二段階の対策を講じる。

①LGWAN 接続系においては、業務用システムとインターネット接続系との通信経路を分割し、両システム間の通信には無害化通信を適用する。

②インターネット接続系においては、不正通信の監視機能の強化等、高度な情報セキュリティ対策を実施することが可能な、ファイアウォールの導入等を行う。

（４）物理的セキュリティ

サーバー室、通信回線及び職員の端末等の管理について、物理的な対策を講じる。

（５）人的セキュリティ

職員が遵守すべき事項を定め、教育及び啓発等を通じて人的対策を講じる。

（６）技術的セキュリティ

コンピューター等の管理、アクセス制御、不正プログラム及び不正アクセス対策等の技術的対策を講じる。

（７）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託におけるセキュリティ確保等、運用面の対策を講じる。また、セキュリティ侵害発生時に迅速かつ適切に対応するため、緊急時対応計画を策定する。

（８）業務委託及び外部サービスの利用

委託事業者の選定、契約への情報セキュリティ要件を明記等、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要な対策の確認及び契約に基づく措置を講じる。

クラウド型サービスの利用に際しては、規定を整備し必要な対策を講じる。

ソーシャルメディアサービスの利用に際しては、運用手順及び発信可能情報を定め、サービスごとの責任者を明確にする。

（９）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を図る。必要に応じて情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて監査及び自己点検を実施する。

8　情報セキュリティポリシーの見直し

監査及び自己点検の結果、または情報セキュリティに関する状況の変化により新たに対策が必要になった場合には、情報及び情報システムに係る脅威の発生の可能性及び損失等を分析し、リスクを検討のうえ、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

上記６から８に規定する対策等を実施するため、具体的な遵守事項及び判断基準等を定める「苫小牧港管理組合情報セキュリティ対策基準に関する要綱」等を策定する。なお、これらの規程は当管理組合の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

附　則

この方針は、令和８年４月１日から施行する。