手取郷広域事務組合情報セキュリティ基本方針

1　目的

本基本方針は、手取郷広域事務組合（以下「組合」という。）が保有する情報資産の機密性、安全性及び可用性を維持するため、組合が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2　定義

本基本方針において使用する用語の定義は、次のとおりとする。

（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等で構成され、処理を行う仕組みをいう。

（3）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。

（4）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう

（5）情報資産

紙、電磁媒体、フイルム等の記録媒体に記録されたすべての情報及び情報システムをいう。

（6）特定個人情報等

組合の取り扱う個人番号及び特定個人情報

（7）機密性

情報にアクセスすることを許可された者だけが、情報にアクセスできる状態を確保することをいう。

（8）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（9）可用性

情報にアクセスすることを認められた者が、必要な時に中断されることなく、情報にアクセスできる状態を確保することをいう。

(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関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11) 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により、コンピューターウイルス等の不正プログラムの付着が無い等、安全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実施する。

（1）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏洩・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洩・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・広範囲にわたる疫病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4　適用範囲

セキュリティポリシーの対象範囲は、次のとおりとする。

（1）対象者

本組合の職員（会計年度任用職員及び臨時的任用職員等を含む）及び当該組合の業務に携わる委託業者とする。

（2）情報資産の範囲

本組合が管理する全ての情報資産

5　職員等の順守義務

職員等は、情報セキュリティの重要性を認識し、業務の遂行に当たってセキュリティポリシー及び関連する法令等を遵守しなければならないものとする。

6　情報セキュリティ対策の実施

上記3に規定する脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）情報セキュリティ管理体制の整備

情報セキュリティ対策を確実にする組合の管理体制を明確にする。

（２）情報資産の明確化及び分類

情報セキュリティ対策を確実及び有効にするために、業務の効率性・利便性の観点を踏まえ、情報資産全体に対し、次の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにしたうえで、端末からの情報持ち出し不可設定等により、住民への情報の流出を防ぐ。

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の高度な情報セキュリティ対策を実施する。

（３）人的セキュリティ対策

情報セキュリティに関する権限と責任を定めるとともに、職員等にセキュリティポリシーの内容を周知徹底するなど、十分な教育及び啓発を行うための必要な対策を講じる。

（４）物理的セキュリティ対策

情報システムを設置する場所への不正な立入、職員等のパソコン等の管理について、情報資産への危害及び妨害等から保護するために物理的な対策を講じる。

（５）技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理、コンピュータウイルス対策等の技術的な対策を講じる。

（６）運用に関するセキュリティ対策

情報システムの監視及びセキュリティポリシー遵守状況の確認等の運用面における必要な対策を行う。また、緊急事態が発生した際に迅速な対応を行うための危機管理対策を講じる。

（７）業務委託と外部サービスの利用

業務委託を行う場合には、情報セキュリティ要件を明記した契約を締結し、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、必要に応じて契約に基づき措置を講じる。

（８）評価及び見直しの実施

情報セキュリティ監査結果等に基づき、情報セキュリティ対策の評価を行うとともに、情報システムの変更、新たな脅威の発生など情報セキュリティを取り巻く状況の変化に対応するために、セキュリティポリシー及び情報セキュリティ共通実施手順の見直しを適宜実施する。

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情報セキュリティ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

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、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、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする

なお、情報セキュリティ実施手順は、公にすることにより組合の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

附則

（施行期日）

この情報セキュリティ基本方針は、令和８年４月１日から施行する。