神奈川県町村情報システム共同事業組合情報セキュリティ基本方針

令和８年３月 23 日　制定

１　目的

本基本方針は、本組合が保有する情報資産の機密性、完全性及び可用性を維持するため、本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

(1)　ネットワーク

コンピュータ等を相互に接続するための通信網及び構成機器(ハードウェア及びソフトウェアを含む。）をいう。

(2)　情報システム

コンピュータ、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。

(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。

①　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保すること。

②　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

③　可用性

情報にアクセスすることを認められた者が、必要なとき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。

(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)　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（所得税及び地方税に関する事務）に関わる情報システム及びデータをいう。

(6)　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。

(7)　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、ウィルス攻撃、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、水害等の災害を要因とする情報資産の漏えい、破壊及び業務の停止等

(4)　大規模・広範囲にわたる疾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

本基本方針の適用範囲は、以下の各号に示すものとする。

(1)　組織

組合内部部局、監査委員及び議会とする。

(2)　情報資産

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　職員等の遵守義務

職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーその他情報セキュリティに関する規程等を遵守しなければならない。

6　情報セキュリティ対策

情報資産を脅威から保護するため、以下の情報セキュリティ対策を講ずる。

(1)　組織体制

本組合の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2)　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、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上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、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) 物理的セキュリティ対策

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ対策

職員等が遵守すべき事項を定め、十分な教育及び啓発が行われるよう必要な対策を講ずる。

(5) 技術的セキュリティ対策

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

(6) 運用セキュリティ対策

① 情報システム等の監視、情報セキュリティポリシーの遵守状況の確認等のため、運用面における必要な対策を講ずる。

② 情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対策を講ずる。

(7) 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、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。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

(8) 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、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜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確保するため、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

情報セキュリティ対策の実施状況の検証の結果又は情報セキュリティに関する状況の変化に対応するため、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。

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。

附　則

この基本方針は、令和８年４月１日から施行する