鹿児島県市町村総合事務組合
情報セキュリティ基本方針

鹿児島県市町村総合事務組合

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

⑴　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，その構成機器（ハードウェア及びソフトウェア）をいう。

⑵　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。

⑶　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。

⑷　情報セキュリティポリシー

本基本方針をいう。

⑸　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をいう。

⑹　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。

⑺　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をいう。

⑻　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務等に関わる情報システム及びデータをいう。

⑼　業務サーバ接続系

業務サーバ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（マイナンバー利用事務系を除く。）。

⑽　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。

⑾　通信経路の分割

業務サーバ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た上で，安全が確保された通信だけを許可できるようにすることをいう。

⑿　無害化通信

危険因子がファイルに含まれていないことを確認し，インターネット接続系から取り込む方式等により，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。

⑬ UTM

ファイアウォール，侵入検知・防御（IDS/IPS），アンチウイルス，Webフィルタリング等の複数のセキュリティ機能を統合して提供する製品（ソフトウェア及びクラウド型サービスを含む。）であって，ネットワーク境界において通信の監視，検知，遮断及び制御を行うものをいう。

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ものとする。

⑴ 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えい・破壊・改ざん・消去，重要情報の詐取，内部不正等

⑵ 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，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

⑶ 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

⑷ 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

⑸ 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

⑴ 行政機関の範囲

本基本方針が適用される行政機関は，管理者，議会，監査委員及び事務局とする。

⑵ 情報資産の範囲

本基本方針が対象とする情報資産は，次のとおりとする。

ア　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

イ　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。）

ウ　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・非常勤職員その他の情報資産，ネットワーク又は情報システムにアクセスすることを認められた者等（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本基本方針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の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ものとする。

⑴　組織体制

本組合の情報資産については，全職員等で情報セキュリティ対策を推進するものとする。

⑵　情報資産の管理

本組合の保有する情報資産について，その機密性，完全性及び可用性に応じて情報セキュリティ対策を実施するものとする。

⑶　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，次の三段階の対策を講じるものとする。

ア　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することにより，情報の流出を防ぐ。

イ　業務サーバ接続系においては，業務サーバと接続する業務用システムと，インターネット接続系の情報システムとの通信経路を分割する。なお，両システム間で通信する場合には，無害化通信を実施する。

ウ　インターネット接続系においては，UTMを用いて不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

⑷　物理的セキュリティ

サーバ，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ものとする。

⑸　人的セキュリティ

情報セキュリティに関し，十分な教育及び啓発を行う等の人的な対策を講じるものとする。

⑹　技術的セキュリティ

UTMを用いて，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よう努めるものとする。

⑺　運用

情報セキュリティポリシーの遵守状況の確認，業務委託を行う際のセキュリティ確保等，情報セキュリティポリシーの運用面の対策を講じるよう努めるものとする。

⑻　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，及び必要に応じて契約に基づき措置を講じるよう努めるものとする。

外部サービス（クラウドサービス）を利用する場合には，情報セキュリティを確保するための対策を講じるよう努めるものとする。

ソーシャルメディアサービスを利用する場合には，利用するソーシャルメディアサービスごとの責任者を定め，情報セキュリティを確保するための対策を講じるよう努めるものとする。

⑼　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，必要に応じて情報セキュリティ監査又は自己点検を実施し，運用改善を行い，情報セキュリティの向上を図るものとする。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ものとする。

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，必要に応じて情報セキュリティ監査又は自己点検を実施するものとする。

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，リスクを検討したうえで，情報セキュリティポリシーを見直すものとする。

附　則

この基本方針は，令和８年４月１日から施行する。