田辺市情報セキュリティ基本方針

１　目的

この基本方針は、本市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、本市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　用語の定義

情報セキュリティポリシーにおける用語の定義は、次の各号に定めるところによる。

⑴　情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

⑵　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。

⑶　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。

⑷　電磁的記録媒体

サーバ装置、端末及び通信回線装置等に内蔵される内蔵電磁的記録媒体と、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ及び磁気テープ等の外部電磁的記録媒体をいう。

⑸　データ等

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。）をいう。

⑹　システム関連文書

システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル及びネットワーク構成図等をいう。

⑺　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。

⑻　機密性

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

⑼　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。

⑽　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、当該

情報にアクセスできる状態を確保することをいう。

⑾　情報セキュリティインシデント

情報資産に対する脅威により、情報セキュリティに関して異常事態が発生したことが明らかになった状態をいう。

⑿　セキュリティ侵害

情報セキュリティインシデントにより、情報資産が侵入、破壊、改ざん及び流出されることをいう。

⒀　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（社会保障、地方税及び防災に関する事務）及び戸籍事務等に関わる情報システム及びデータをいう。

⒁　ＬＧＷＡＮ接続系

ＬＧＷＡＮ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。）。

⒂　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。

⒃　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。

⒄　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。

⒅　職員

本市に在職する地方公務員法（昭和25年法律第261号）第３条に規定する一般職及び特別職の職員のうち、情報資産を使用する職員

３　対象とする脅威

情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

⑴　不正アクセス、ウイルス攻撃及び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、重要情報の詐取及び内部不正等

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、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及び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、通信の途絶及び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　組織の範囲

情報セキュリティポリシーが適用される行政機関は、市長部局、会計課、議会事務局、消防本部、水道部及び各行政委員会の部署並びに本市の管理する情報システムの利用に当たって必要な措置を講じなければならない者とする。

⑵　情報資産の範囲

情報セキュリティポリシーの対象となる情報資産は、次のとおりとする。ただし、「教育学習に利用するネットワーク」及び「医療情報系ネットワーク」を除く。

ア　ネットワーク
イ　情報システム
ウ　ネットワーク及び情報システムに関する施設・設備
エ　電磁的記録媒体
オ　データ等
カ　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の共通の認識を持ち、業務の遂行に当たっては、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の脅威から本市の情報資産を保護するため、次に掲げる情報セキュリティ対策を講じる。

⑴　組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

⑵　情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

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、マイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系の３つの系統に応じ

た対策を講じる。

ア　マイナンバー利用事務系においては、原則として、他の領域との通信が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、住民情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮ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、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。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

⑷　物理的セキュリティ

サーバ、サーバ室、通信回線及び職員のパソコン等の管理について、物理的な対策を講じる。

⑸　人的セキュリティ

情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

⑹　技術的セキュリティ

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及び不正アクセス対策等の技術的な対策を講じる。

⑺　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ものとする。また、情報資産に対する脅威が発現した場合等に迅速かつ適正に対応するため、緊急時における対応に関する計画を策定する。

⑻　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、受託事業者を選定した上で情報セキュリティ要件を明記した契約を締結し、受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するとともに、必要に応じて契約に基づき措置を講じる。

この場合において、外部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。また、ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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、情報セキュリティポリシーを見直すこととする。

9　情報セキュリティ対策基準の策定

上記６から８まで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本市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。