第１章　情報セキュリティ基本方針

１　目的

本市が取り扱う情報資産には、市民の個人情報を始めとし行政運営上重要な情報など部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害事故等から防御することは、市民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

さらに、市民サービスの向上、業務効率化や合理化の要請に対応するために、本市における情報システムによる業務量及び利用範囲は拡大の一途をたどっており、今や行政運営基盤として欠かせないものとなっている。そのため、本市の業務執行を今後も円滑に進めるためには、本市が管理している全ての情報システムが高度な安全性を有することが不可欠である。

このため、本市の情報資産の機密性、完全性及び可用性を維持するため、情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。このうち情報セキュリティ基本方針においては、本市の情報セキュリティ対策及び個人情報の取扱いに関する基本的な方針として、情報セキュリティポリシーの適用範囲、位置付け等を定めるものとする。本市の情報資産を利用する職員は、情報セキュリティの重要性を認識し、この情報セキュリティ基本方針を遵守しなければならない。

２　定義

（１）　コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

（２）　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。

（３）　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。

（４）　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。

（５）　情報資産

情報システムで取り扱う情報で、開発及び運用に係るものを含むすべての情報をいう。

（６）　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。

（７）　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。

（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。

(10) 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、地方税若しくは防災に関する事務)又は戸籍事務等に関わる情報システム及びデータをいう。

(11) 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。)。

(12) 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。

(13) 独立系

上記(１０)、(１１)、(１２)の要件に該当しない情報システムが接続する共用ネットワーク、当該情報システム専用のネットワーク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。

(14) 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。

(15) 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。

(16) 外部サービス

クラウドサービス、Web 会議サービス、SNS 等、庁外の通信回線やシステムを利用して委託業者等が提供するサービスをいう。

(17) クラウドサービス

クラウドサービスは、ソフトウェア・データ・サーバなどをネットワーク経由で利用する仕組みの総称をいう。

(18) クラウドサービス事業者

クラウドサービスを提供し、本市と利用における契約をした組織をいう。また、本市と契約前のクラウドサービス事業者のことをクラウドサービス提供者という。

３ 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本市の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高

位に位置するものである。

4　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・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

（6）　その他、本市の情報資産の機密性、完全性及び可用性を脅かす脅威

5　適用範囲

情報セキュリティポリシーの適用範囲は、以下に示すものとする。

（1）　行政機関等の範囲

本基本方針が適用される行政機関等は、市長部局、議会、行政委員会、各公営企業及びその他本市に属する機関とする。

（2）　情報資産の範囲

本基本方針が適用される情報資産は、上記(1)の行政機関等が所掌する次のとおりとする。

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

④　紙書類やデータなどの状態、記録媒体に限らず、組織内にある全ての情報

（3）　対象者

上記(2)の情報資産に接する組織の職員(会計年度任用職員及び臨時的任用職等を含む。以下「職員等」という。)とする。

6　職員等の遵守義務

職員等は､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、情報セキュリティ実施手順及び個人情報保護制度運用の

手引を遵守しなければならない。

7　情報セキュリティ対策

上記４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。

（１）　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。

（２）　情報資産の分類と管理

本市の保有する情報資産を重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３）　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。

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、住民情報の流出を防ぐ。

②　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。

③　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する宮崎県自治体情報セキュリティクラウドに参加する。

（４）　物理的セキュリティ

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。

（５）　人的セキュリティ

情報セキュリティに関し、職員等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。

（６）　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、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、緊急時対応計画を策定する。

（8） 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。

職務としてソーシャルメディアサービスを利用する場合には、「小林市職員のソーシャルメディア利用ガイドライン」を定め、運用手順を規定する。

（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。

8 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。

9 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。

10 情報セキュリティ対策基準の策定

上記７、８及び９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。

11 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。