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おり、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、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すべ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（注）を維持するための対策を整備するため、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の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（IS07498-2:1989）

機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確保にすること。

完全性（integrity）：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。

可用性（availability）：許可された利用者が必要な時に情報にアクセスできることを確保すること。

２　定義

（１）　部等

対馬市部設置条例（平成１７年対馬市条例第２号）第１条に掲げる部、会計課、教育委員会事務局、監査委員事務局、農業委員会事務局、議会事務局、選挙管理委員会事務局、消防署、消防本部及び各公営企業をいう。

（２）　事務所管課

その保有するデータの一部又は全部の電子計算機処理を行うことにより所管する事務を遂行する課（これに準ずるものを含む。以下同じ。）をいう。

（３）　電子計算機

ハードウェア及びソフトウェアで構成するコンピュータをいう。電子計算機のうち、職員等が情報処理を行うために直接操作する機器を端末といい、そのうち、必要に応じて移動させて使用することを目的として導入したものをモバイル端末という。また、モバイル端末のうち、庁舎内と同様の汎用的業務を庁舎外で行うために使用するものをテレワーク端末という。

（４）　記録媒体

電子計算機に使用される電磁的記録媒体をいう。記録媒体のうち、取り外し可能で持ち出し可能なものを外部記録媒体という。

（５） 電子計算機室等

本市の電子計算機（端末を除く。）を運用管理する目的で設置している部屋をいう。

（６） ネットワーク

電子計算機等を相互に接続するための通信回線及び、その構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

（７） 情報システム

電子計算機、ネットワーク、周辺機器等の組み合わせ、又は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。情報システムが接続するネットワークは以下ものをいう。

① マイナンバー利用事務系（個人番号利用事務系）ネットワーク

個人番号利用事務を取り扱う情報システムが接続する共用ネットワーク及び当該情報システム専用のネットワークをいう。

② ＬＧＷＡＮ接続系ネットワーク

ＬＧＷＡＮに接続する共用ネットワーク及びＬＧＷＡＮに接続する情報システム専用のネットワークをいう（個人番号利用系事務を除く。）。

③ インターネット接続系ネットワーク

インターネットにアクセス又はインターネットからのアクセスを許可する情報システムが接続するネットワークをいう。

④ 独立系ネットワーク

上記の①から③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及び情報システム専用のネットワークをいう。

（８） 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。

（９） 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ない等、安全が確保された通信をいう。

（１０） 行政情報

本市の行政事務の執行に関わる情報で、情報システムで取り扱うものをいう（入出力帳票及び情報システム仕様書等も含む。）。ただし、行政情報を外部に提供した場合やＩＣカード等に行政情報を記録したものを市民に交付する等により、当該情報の管理責任が本市から離れたものを除く。

（１１） 情報資産

本市の情報システム、外部記録媒体及び行政情報をいう。

（１２） 特定用途機器

テレビ会議システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵の記録媒体を備えているものをいう。

（１３） ロボティック・プロセス・オートメーション

ロボティック・プロセス・オートメーション（以下「ＲＰＡ」という。）はこれまで人間が行ってきた定型的な処理等をソフトウェアのロボットにより自動化するものをいう。

（１４） 外部サービス

外部サービスとは、事業者が提供するサービスの総称であり、以下のものをいう。

① 委託による外部サービス

本市の業務を事業者に委託することにより調達する外部サービスのことをいう。

② 約款等による外部サービス

有料、無料を問わず以下の形態により調達する外部サービスのことをいう。

ア 約款への同意のみにより利用可能となる外部サービス

事業者が定める約款への同意によって利用可能となるサービスのことをいう。

イ 国が提供する外部サービス

国が運営し、提供するサービスのことをいう。

ウ ガバメントクラウド

政府の情報システムについて、共通的な基盤・機能を提供する複数のクラウドの利用環境のことをいう。ガバメントクラウドは、マイナンバー利用事務系と同一とみなして利用可とする。

（１５） クラウドサービス

データやソフトウェアをネットワーク経由でサービスとして利用者に提供するものをいい、主に仮想化技術により実現されているものをいう。

（１６） 仮想化技術

サーバなどのハードウェア資源（ＣＰＵ、メモリ、ディスクなど）を抽象化し、物理的な制限にとらわれず、ソフトウェア的に統合・分割できるようにする技術のことをいう。

（１７） テレワーク

情報通信技術（ＩＣＴ＝Ｉｎｆｏｒｍａｔｉｏｎ ａｎｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ）を活用した勤務場所にとらわれない柔軟な働き方のことをいう。

（１８） 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。

（１９） 情報セキュリティインシデント

情報セキュリティインシデントとは、本市の情報資産に対する脅威が実際に生じることにより、情報資産の機密性、完全性又は可用性が損なわれることであり、以下ものをいう。

ア 情報システムの故障、停止

イ　情報システムへの不正アクセス攻撃
ウ　情報システムの不正な利用
エ　情報システムにおける入出力内容の誤り
オ　情報資産の盗難
カ　情報資産の紛失、滅失
キ　行政情報の漏えい
ク　行政情報の改ざん
ケ　行政情報の誤送付、誤送信
コ　その他の障害

（２０）　ソーシャルメディア

ブログ、ソーシャルネットワーキングサービス（ＳＮＳ）、動画共有サイト等、利用者が情報を発信し、形成していくメディアのことをいう。

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　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は、本市の部等における情報資産及び情報資産に接するすべての職員（非常勤職員、会計年度任用職員及び再任用職員を含む。以下同じ。）とする。

５　職員の義務

職員は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用に当たっては情報セキュリティポリシーを遵守しなければならない。

６　情報セキュリティの管理体制

本市の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

７　情報資産の分類

情報資産をその重要度に応じて分離し、それに応じたセキュリティ対策を行うものとする。

８　情報資産への脅威

情報セキュリティ対策を講ずるうえで、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に以下の脅威については十分な措置を講ずるものとする。

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、重要情報の搾取、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、落雷並びに火災等の災害や事故、故障等

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

9 情報セキュリティの対策

本市の情報資産を上記８の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ものとする。

（1） 人的セキュリティ対策

情報資産に接する職員の情報セキュリティに関する権限や責任等を定めるとともに、すべての職員に情報セキュリティポリシーの内容を周知徹底するため、教育及び訓練を行う。

（2） 物理的セキュリティ対策

電子計算機、通信回線、外部記録媒体等の管理及び電子計算機室等について不正な立入り等から保護するため、入退室や機器管理上の物理的な対策を講ずる。

（3） 技術的セキュリティ対策

情報資産を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、コンピュータウイルス対策等を実施する。

（4） 運用

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、ネットワークの監視等の運用面における必要な措置を講ずる。

また、情報資産に対するセキュリティ侵害が発生した際の迅速な対応と行政事務の円滑な執行を可能とするため、必要な措置を講ずるものとする。

１０ 情報セキュリティ対策基準の策定

本市の情報セキュリティ基本方針を実行に移すため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

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。情報セキュリティ実施手順は、本市全体として遵守すべき事項を規定したものと、重要な情報システムの適切な運用に関する事項を規定したものを策定する。

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。

１２　評価・見直し

（1）　監査及び自主点検の実施・見直し

情報セキュリティポリシーの順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主点検を実施する。

（2）　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主点検の結果、情報セキュリティポリシーの見直しが必要に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、情報情報セキュリティポリシーを見直す。