島本町情報セキュリティポリシー

（平成２８年　１月　１日）
最近改正　令和　７年１０月　１日

序章　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、島本町が保有する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定めるものである。

情報セキュリティポリシーは、情報資産に関する業務に携わる本町の全職員に浸透、普及並びに定着させるものであり、安定的な規範であることが要請される。一方、情報技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）の２階層に分けて策定するものとする。

また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順として、「情報セキュリティ実施手順」を策定することとする。

情報セキュリティポリシーの構成

構　　成		内　　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

第１章　情報セキュリティ基本方針

１　目的

島本町の各情報システムが取扱う情報には、住民の個人情報のみならず行政運営上重要な情報、外部に漏えいした場合には極めて重大な結果を招く情報が含まれている。

したがって、これらの情報等を、人的脅威、災害、事故等の様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、安全かつ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。

ついては、このことが本町に対する住民からの信頼の維持向上に寄与するものである。

そのため、島本町の情報資産の機密性、完全性及び可用性を維持するための対策を整備するために島本町情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については、本町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。

2　定義

⑴ 職員等

特別職の職員（町長、副町長及び教育長に限る。）及び一般職の職員並びに町立学校等に勤務する府費負担教職員をいう。

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 サーバ室

情報システムを集約して設置し、管理している部屋をいう。

⑸ 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。

⑹ 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。

⑺ 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。

⑻ 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。

⑼ 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、地方税又は防災に関する事務）又は戸籍事務等に係る情報システム及びデータをいう。

⑽ 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。）。

⑾ インターネット接続系

インターネットメール又はＣＭＳに係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。

⑿ 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。

⒀ 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。

⑭ 端末

デスクトップパソコン、ノートパソコン、モバイル端末等の業務に利用する端末のことをいう。

3　対象とする脅威

情報資産に対する脅威として、特に認識すべきものとして次の脅威を想定し、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、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 情報資産の無断持出し、許可していないソフトウェアの使用等の規定違反、設計・開発の不備、操作・設定ミス、メンテナンス不備、外部委託管理の不備、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障害からの波及等

4　適用範囲

⑴ 行政機関の範囲

本ポリシーが適用される行政機関は、島本町の全ての機関とする。

なお、島本町の情報資産に係る業務を外部に委託する場合又は指定管理者に実施させる場合は、当該業務の受託者又は指定管理者等の関係者も含むものとする。(ただし、町立学校において教育用に使用するものは除く。)

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。

① ネットワーク、情報システム及びこれらに関する設備、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

職員等は、情報セキュリティの重要性を認識するとともに、業務の遂行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　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

⑴ 組織体制

本町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及び役割を確立する。

⑵ 情報資産の分類及び管理

情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に応じた情報セキュリティ対策を行う。

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３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対策を実施する。

⑷ 物理的セキュリティ

サーバ、情報システムを設置する部屋、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。

⑸ 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。

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、不正アクセス対策等の技術的対策を講じる。

⑺ 運用

情報セキュリティポリシーの遵守状況の確認、外部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切に対応するため、緊急時対応計画を策定する。

⑻ 業務委託と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。

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。

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、定期的に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新たに対策が必要になった場合等には、情報セキュリティポリシーを見直す。

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。

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町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。