飛島村情報セキュリティポリシー

令和８年４月

飛島村
飛島村教育委員会
飛島村議会
飛島村監査委員
飛島村固定資産評価審査委員会
飛島村選挙管理委員会
飛島村農業委員会

改訂履歴

番号	制定改訂日	内容
００	平成 15 年８月	新規規定
０１	平成 21 年３月３日	部分改訂
０２	平成 25 年４月１日	部分改訂
０３	平成 27 年４月１日	部分改訂
０４	令和２年４月１日	部分改訂
０５	令和６年４月１日	部分改訂
０６	令和７年３月１日	部分改訂
０７	令和８年４月１日	部分改訂

第1章　情報セキュリティ基本方針

1　目的

近年、情報通信技術の進歩により企業活動や個人の生活スタイルに情報システムは必要不可欠な存在になっている。このいわゆるIT革命は、地方公共団体の行政活動にも大きな影響を与えることとなり、本村も例外ではなく、継続的かつ安定的な行政サービスを提供するために、行政事務の大半を各情報システムに依存しているのが現状である。

本村の各種情報システムが取り扱う情報には、個人情報はもちろん、行政運営上重要な情報など、部外に漏洩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。

LGWANや電子自治体構想など、地方自治体に更なるＩＣＴ化が求められていく中、今後も行政サービスを提供し続けるためには、適切な情報セキュリティ対策を実施することで、本村が所有する情報及びその情報を取り扱う情報システムをあらゆる脅威から防御することが必要となってきている。

このため、情報セキュリティ対策の包括的な規定として、情報セキュリティポリシーを（以下、ポリシー）策定し、管理範囲内での各種情報資産の機密性、完全性、可用性を維持し、情報セキュリティの確保に最大限取り組むものとする。

2　用語及び定義

○　情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

○　情報資産

飛島村で情報を取り扱うための資産であり、ハードウェア、ソフトウェア、データ資産及びサービスをいう。

○　データ資産

文字、符号、数値、図画、写真等が記録された電子情報及び紙情報をいう。

○　電子情報

電磁的情報及びディスプレイに表示された可視的情報をいう。

○　紙情報

プリンタ・プロッタ・コピー機等を用いて紙媒体に印刷された可視的情報及び紙媒体に手書きで記入された可視的情報をいう。

○　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網、その構成機器（ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

○　情報システム

庁舎及び関係施設内において、業務系の電子計算機（業務系におけるネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

○　記録媒体

情報を記録するために使用される電子媒体及び紙媒体をいう。

○　電子媒体

MO（光磁気ディスク）、FD（フロッピーディスク）、CD（コンパクトディスク）、DVD（ディーブイディー）、BD（ブルーレイディスク）、USB メモリ、コンパクトフラッシュ、SD カード等の磁気や光学式による記録に使用する媒体をいう。

○　紙媒体

手書き又はプリンタ・プロッタ・コピー機等を用いて印刷するときに、記録するために使用する媒体をいう。

○　情報セキュリティポリシー

飛島村が所有する情報資産の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。

どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定で、情報セキュリティ基本方針及び情報セキュリティ対策基準からなるもの。ただし、情報セキュリティ基本方針に限り、飛島村事務分掌規則（平成８年規則第１号）の規定に基づき設置される組織、飛島村会計管理者の補助組織設置規則（昭和５７年規則第１７号）の

規定に基づき設置させる組織、飛島村教育委員会事務局等組織規則（平成１３教委規則第１号）の規定に基づき設置される組織、飛島村議会事務局処務規程（昭和５７年議会規程第２号）の規定に基づき設置される組織及び地方自治法（昭和２２年法律第６７号）第２００条第２号に基づく監査委員事務局、地方自治法第８９条の規定に基づき設置させる議会、地方自治法第１９５条第１項に規定する監査委員、地方税法（昭和２５年法律第２２６号）第４２３条第１項に規定する固定資産評価審査委員会、地方自治法第１８１条の規定に基づき設置される選挙管理委員会、農業委員会等に関する法律（昭和２６年法律第８８号）第３条第１項に基づき設置される組織並びにその他これらの規定に基づき設置される組織に準ずる組織のうち、村長が認める組織に適用するものとする。

○　職員等

雇用の形態や職位にかかわらず、また飛島村の業務に定期従事するかにかかわらず、村が所管する情報資産を取り扱う正規職員、会計年度任用職員、臨時職員等をいう。

なお、村長、副村長及び教育長を含むものとする。

○　庁舎外

飛島村の施設内以外の場所をいう。例えば、以下の①～⑥が該当する。

①　村民宅
②　国、県、他の市区町村
③　協議会や外郭団体、農協、学校、病院
④　職員等の自宅
⑤　委託事業者
⑥　その他村の施設以外

○　特定用途機器

テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリング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り、通信回線に接続されている又は電磁的記録媒体を内蔵しているものをいう。

○　クラウドサービス

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でア

クセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service Service）、PaaS（Platformas a Service Service）、IaaS（Infrastructure as a Service Service）等がある。

＜クラウドサービスの例＞

・仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
・データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
・Web 会議サービス
・SNS（ソーシャルメディア）
・検索サービス、翻訳サービス、地図サービス

3　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、本村が所有又は管理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、体系的に取りまとめたものであり、情報セキュリティ対策の最上位に位置するものである。

したがって、本村が所掌する情報資産に関する業務に携わる職員等及び委託事業者はポリシーの実施に責任を負うとともに、これを尊重し、遵守しなければならない。

4　情報セキュリティ管理体制

本村の情報資産について、課長等（飛島村事務分掌規則第３条に定める課長等及び会計管理者、議会事務局長並びに飛島村教育委員会等組織規則第６条に定める課長職以上の職にある者が率先して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。

5　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6　情報資産への脅威

情報セキュリティポリシーを遵守する上で、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。

特に認識すべき脅威は、以下のとおりである。

①　権限外者による故意の不正アクセス又は不正操作によるデータやプロ

グラムの持出・盗聴・改ざん・消去等、機器及び記録媒体の盗難等

② 職員等又は委託事業者によるデータやプログラムの持出・盗聴・改ざん・消去等、機器及び記録媒体の盗難等、規定外の情報システムの機器操作によるデータ漏洩等

③ コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

7 情報セキュリティ対策

本村の情報資産を上記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 組織・体制

情報セキュリティの確保のため、幹部が率先して推進・管理することで組織全体が情報セキュリティ対策を推進できる体制を確立し、その責任及び権限を明確にする。

② 情報の管理

情報システムにおいて取扱う情報について、重要な情報を重点管理する考え方から、重要度に応じた情報分類を行い、その重要度に応じた情報セキュリティ対策を規定する。

③ 物理的セキュリティ

情報システムの設置場所に関して、不正な立入り、損傷及び妨害等から情報資産を保護するための物理的な対策を規定する。

④ 人的セキュリティ

情報セキュリティに関する権限や責任について規定する。また、情報セキュリティの向上は、情報資産の利便性の向上とは必ずしも相容れないものであり、職員の理解が得にくい場合もあるので、情報セキュリティについての十分な教育及び啓発が講じられるように必要な対策を規定する。

⑤ 技術的セキュリティ及び運用

情報資産を外部からの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、ネットワーク管理等の技術的対策を規定する。更に、ポリシーの実効性を確保するため、業務委託を含めたポリシーの遵守状況の確認、ネットワークの監視等の運用面に関して必要な措置を規定する。また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

⑥ 法令遵守

情報システム等の利用に際しては、ポリシーに従うだけでなく法律等

を侵すことのないよう配慮すべきことを確認するため、法令遵守を規定する。

⑦　情報セキュリティに関する違反に対する対応

ポリシーの実効性を担保するために情報セキュリティに関する違反行為に対する対応を規定する。

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。

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。

⑨　評価・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。

8　情報セキュリティ対策基準の策定

本村の様々な情報資産について、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、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。

9　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を具体的に実施していくためには、個々の情報資産に対応した実施手順等を定めていく必要がある。そのため、上記により定めた情報セキュリティ対策基準の基本的な要件に基づき、課長等が所掌する情報資産の情報セキュリティ実施手順を策定するように努める。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより飛島村の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。