美浦村情報セキュリティポリシー

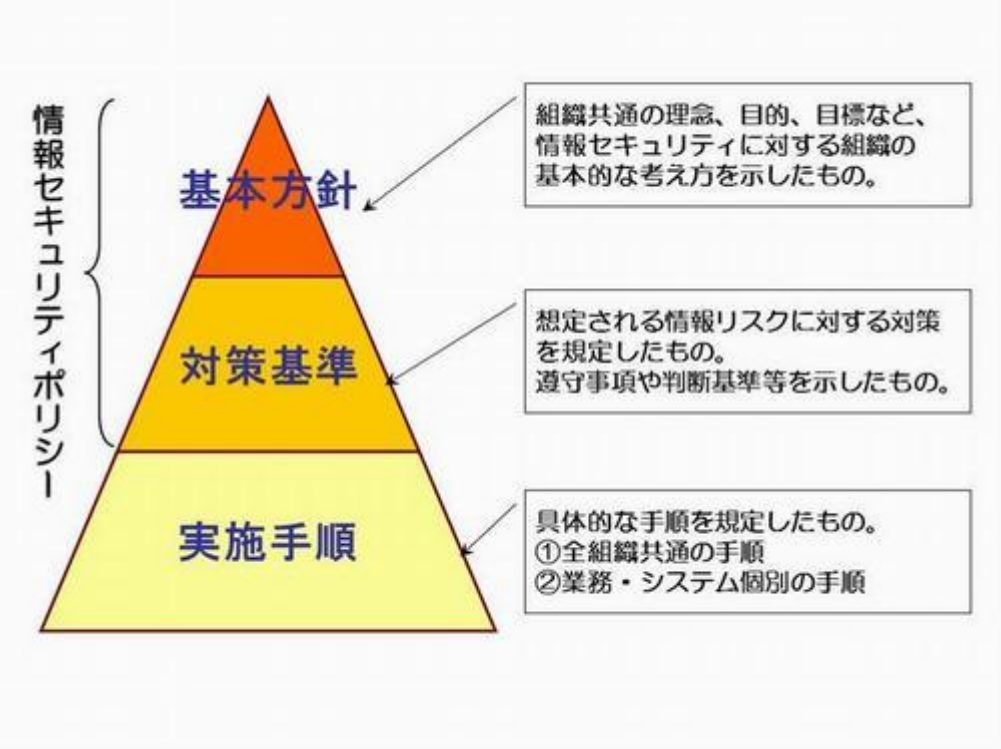
平成14年 4月1日 策　　定
平成19年 4月1日 全部改定
平成24年 4月1日 一部改定
平成27年10月5日 全部改定

美浦村情報セキュリティポリシーの構成

美浦村情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、美浦村が保有する情報資産に関する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る。

情報セキュリティポリシーは、本村の情報資産を取扱う全職員に浸透、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。しかし一方では、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、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は、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層のものとして構成する。また、情報セキュリティポリシーに基づく具体的な手順を示す「情報セキュリティ実施手順」として全庁的に共通する情報資産の取扱いを定める実施手順と，管理する情報システム毎の取扱いを定める実施手順を策定するものとする。



美浦村情報セキュリティポリシーの構成

また、近年の情報化の急激な普及により、電子自治体の構築が期待されているところである。美浦村がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、美浦村の情報資産の機密性、完全性、可用性、及び正当性を維持するための対策（情報安全対策）として情報管理基本方針と情報管理対策基準を定める。このうち、情報管理基本方針については美浦村の情報管理対策の基本的な方針として、情報安全対策の意義、対象等を定めるものとする。

情報セキュリティ基本方針

基本的な考え方

美浦村（以下「本村」という）は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報のみならず、行政運営上重要な情報等を多数保有するとともに、ほかに代替することができない行政サービスを提供している。このため、本村が取扱う情報が、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。

インターネットその他の高度情報通信ネットワークの整備及び情報通信技術を活用することで、電子自治体が進展している今日、業務の多くが情報システムやネットワークに依存しており、情報システムからの情報漏えい、停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。

地方公共団体は相互にネットワーク接続しており、発生したIT 障害がそのネットワークを介して他の団体に連鎖的に拡大する可能性は否定できない。

そのため、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下、「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

従って、これらの情報及び情報を取扱う情報システムを様々な脅威から、住民の財産、プライバシー等を守るためにも、また、業務継続のためにも、その対策は、必要不可欠である。

また、情報セキュリティ対策は、個人情報保護対策と内容的に重なる部分も多く、自然災害時や大規模・広範囲にわたる疾病における対応という意味では防災対策とも重なる。

ついては、情報セキュリティを対策する部署とこれらを担当する部署は、相互に連携をとって、それぞれの対策に取り組むことが求められる。

村がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件であり、ひいては、このことが本村に対する住民からの信頼の維持向上と安全で安心して暮らせるまちづくりに寄与するものである。

1. 目的

本基本方針は、本村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、本村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. 定義

（1） 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(ハードウエア及びソフトウエア) をいう。

（2） 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。

（3） 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。

（４） 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。

（５） 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。

（６） 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。

（７） 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。

3. 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、外部委託管理の不備、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

4. 適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

（２）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. 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。

したがって、本村が保有する情報資産に接するすべての職員（非常勤職員及び臨時職員を含む。）及び契約により操作等を認められた外部委託者は、情報セキュリティポリシーについて共通の認識を持つとともに、情報セキュリティポリシーを遵守する義務を負うものとする。

6. 職員等の遵守義務

職員、非常勤職員及び臨時職員（以下「職員等」という。）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。

7. 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、以下の情報セキュリティ対策を講じる。

（１）組織体制

本村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

本村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行う。

（３）物理的セキュリティ

サーバ等、情報システム室等、通信回線等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。

（４）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。

（５）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。

（６）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、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。

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、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。

なお、情報セキュリティ対策基準は、公にすることにより本村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。

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村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。

情報セキュリティ委員会組織体制

最高情報統括責任者（CIO）	副村長
最高情報セキュリティ責任者（CISO）	副村長
統括情報セキュリティ責任者	情報政策担当部長
情報セキュリティ責任者	上記以外の部長
情報セキュリティ管理者	各課局園所長
情報システム管理者	システム所管の課長

情報セキュリティポリシー対策チーム

部署	選定の理由
情報政策担当課	庁内業務の情報政策の主管
情報システム担当課	庁内の情報システムの主管
総務担当課	個人情報保護条例の主管
文書担当課	文書管理システム規程、文書管理規程システムの主管
防災担当課	災害等の危機管理の主管
施設管理担当課	庁内の施設管理の主管
広報担当課	報道機関への対応の主管